501.42780X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	AIKAWA, et al.
Serial No.:	Not assigned
Filed:	June 25, 2003
Title:	SMART CARD AND SETTLEMENT TERMINAL
Group:	Not assigned

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

June 25, 2003

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanese Application No.(s) 2002-220602 filed July 30, 2002.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No. 29,621

CIB/amr
Attachment
(703) 312-6600

日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年　７月３０日

出願番号
Application Number:　特願２００２－２２０６０２

[ST.10/C]:　[ＪＰ２００２－２２０６０２]

出願人
Applicant(s):　株式会社日立製作所

２００３年　３月１４日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０１６５３５

【書類名】　特許願

【整理番号】　D02001851A

【あて先】　特許庁長官殿

【国際特許分類】　H04L　9/14

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区吉田町２９２番地　株式会社日立製作所デジタルメディア開発本部内

【氏名】　相川　慎

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区吉田町２９２番地　株式会社日立製作所デジタルメディア開発本部内

【氏名】　高見　穣

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区吉田町２９２番地　株式会社日立製作所デジタルメディア開発本部内

【氏名】　福島　真一郎

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　　要約書　1

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　ICカードおよび決済端末

【特許請求の範囲】

【請求項１】外部と通信する通信手段と、データやプログラムを蓄積する情報蓄積手段と、情報処理を行う演算処理手段を有するICカードにおいて、

前記情報蓄積手段は、価値データと、前記価値データを更新するために使用する転送鍵と、前記転送鍵の新旧を値の大小で識別する転送鍵識別子と、前記転送鍵を更新するために使用する更新鍵と、前記ICカードが格納可能な前記転送鍵識別子の上限値を表す転送鍵識別子上限値を保存し、

前記演算処理手段は、前記更新鍵を用い、共通鍵暗号方式に基づいた暗号処理を行うことで、前記転送鍵識別子と前記転送鍵を更新する処理を行い、

その後、前記転送鍵を用い、共通鍵暗号方式に基づいた暗号処理を行うことで、前記価値データを更新する処理を行うことを特徴とするICカード。

【請求項２】前記演算処理手段は、

カード情報の送信を要求するコマンドデータを受信した時は、前記転送鍵識別子を、レスポンスデータとして外部に送信する処理を行い、

前記転送鍵の更新許可を要求するコマンドデータを受信した時は、第１の乱数を生成して、前記第１の乱数をレスポンスデータとして外部に送信する処理を行い、

前記転送鍵の取得を要求し、第２の乱数を格納しているコマンドデータを受信した時は、前記第２の乱数と、前記転送鍵識別子と、前記転送鍵を、共通鍵暗号方式に基づき、前記更新鍵で暗号化した、第１の暗号化データを、レスポンスデータとして外部に送信を行い、

前記転送鍵の更新を要求し、第２の暗号化データを格納しているコマンドデータを受信した時は、前記第２の暗号化データを、共通鍵暗号方式に基づき、前記更新鍵で復号化して、第１のデータと、第２のデータと、第３のデータを抽出し、前記第１のデータが前記第１の乱数と等しく、且つ、前記第２のデータの値が、前記転送鍵識別子上限値と前記転送鍵の値の間に含まれるならば、前記転送鍵識別子の値を前記第２のデータの値に書き換えるとともに、前記転送鍵の値を前記

第３のデータの値に書き換える処理を行うことを特徴とする請求項１記載のICカード。

【請求項３】外部と通信する通信手段と、データやプログラムを蓄積する情報蓄積手段と、情報処理を行う演算処理手段を有するICカードにおいて、

前記情報蓄積手段は、価値データと、前記価値データを更新するために使用する転送鍵と、前記転送鍵の新旧を値の大小で識別する転送鍵識別子と、前記転送鍵を更新するために使用する第１の公開鍵を含んだ第１の公開鍵証明書と、前記第１の公開鍵に対応した秘密鍵と、前記ICカードが格納可能な前記転送鍵識別子の上限値を表す転送鍵識別子上限値を保存し、

前記演算処理手段は、前記第1の公開鍵証明書と前記秘密鍵を用いて、公開鍵暗号方式に基づいた暗号処理を行うことで、前記転送鍵識別子と前記転送鍵を更新する処理を行い、

その後、前記転送鍵を用い、共通鍵暗号方式に基づいた暗号処理を行うことで、前記価値データを更新する処理を行うことを特徴とするICカード。

【請求項４】前記演算処理手段は、

カード情報の送信を要求するコマンドデータを受信した時は、前記転送鍵識別子と、前記第１の公開鍵証明書を、レスポンスデータとして外部に送信する処理を行い、

前記転送鍵の更新許可を要求し、第２の公開鍵を含んだ第２の公開鍵証明書を格納しているコマンドデータを受信した時は、第１の乱数を生成して、前記第１の乱数をレスポンスデータとして外部に送信する処理を行い、

前記転送鍵の取得を要求し、第３の公開鍵を含んだ第３の公開鍵証明書と、第２の乱数を格納しているコマンドデータを受信した時は、まず、前記転送鍵識別子と、前記転送鍵を、公開鍵暗号方式に基づき、前記第３の公開鍵で暗号化した第１の暗号化データを作成し、次に、前記第１の暗号化データと、前記第２の乱数から、公開鍵暗号方式に基づき、前記秘密鍵で、第１のデジタル署名データを作成し、最後に、前記第１の暗号化データと、前記第１のデジタル署名データを、レスポンスデータとして外部に送信する処理を行い、

前記転送鍵の更新を要求し、第２の暗号化データと、第２のデジタル署名データ

を格納しているコマンドデータを受信した時は、まず、前記第２のデジタル署名データを、公開鍵暗号方式に基づき、前記第２の公開鍵で検証し、次に、前記第２の暗号化データを、公開鍵暗号方式に基づき、前記秘密鍵で復号化して、第１のデータと、第２のデータを抽出し、最後に、前記第1のデータの値が、前記転送鍵識別子上限値と前記転送鍵の値との間に含まれるならば、前記転送鍵識別子の値を前記第1のデータの値に書き換えるとともに、前記転送鍵の値を前記第２のデータの値に書き換える処理を行うことを特徴とする請求項３記載のICカード。

【請求項５】外部と通信する通信手段と、データやプログラムを蓄積する情報蓄積手段と、情報処理を行う演算処理手段を有するICカードにおいて、

前記情報蓄積手段は、価値データと、前記価値データを更新するために使用する転送鍵と、前記転送鍵の新旧を値の大小で識別する転送鍵識別子と、前記転送鍵を更新するために使用する更新鍵と、前記更新鍵の新旧を値の大小で識別する更新鍵識別子と、前記転送鍵を更新するために使用する第１の公開鍵を含んだ第１の公開鍵証明書と、前記第１の公開鍵に対応した秘密鍵と、前記ICカードが格納可能な前記転送鍵識別子の上限値を表す転送鍵識別子上限値を保存し、

前記演算処理手段は、前記更新鍵を用い、共通鍵暗号方式に基づき、前記転送鍵の更新を行うか、

あるいは、前記第1の公開鍵証明書と前記秘密鍵を用い、共通鍵暗号方式に基づき、前記転送鍵の更新を行い、

その後、前記転送鍵を用い、共通鍵暗号方式に基づいた暗号処理を行うことで、前記価値データを更新する処理を行うことを特徴とするICカード。

【請求項６】前記演算処理手段は、

カード情報の送信を要求するコマンドデータを受信した時は、前記転送鍵識別子と、前記更新鍵識別子と、第1の前記公開鍵証明書を、レスポンスデータとして外部に送信する処理を行い、

前記転送鍵の更新許可を要求するコマンドデータを受信した時は、第１の乱数を生成して、前記第１の乱数をレスポンスデータとして外部に送信する処理を行い、

前記転送鍵の取得を要求し、第２の乱数を格納しているコマンドデータを受信した時は、前記第２の乱数と、前記転送鍵識別子と、前記転送鍵を、共通鍵暗号方式に基づき、前記更新鍵で暗号化した、第１の暗号化データを、レスポンスデータとして外部に送信する処理を行い、

前記転送鍵の更新を要求し、第２の暗号化データを格納しているコマンドデータを受信した時は、まず、前記第２の暗号化データを、共通鍵暗号方式に基づき、前記更新鍵で復号化して、第１のデータと、第２のデータと、第３のデータを抽出し、次に、前記第１のデータが前記第１の乱数と等しく、且つ、前記第２のデータの値が、前記転送鍵識別子上限値と前記転送鍵の値との間に含まれるならば、前記転送鍵識別子の値を前記第２のデータの値に書き換えるとともに、前記転送鍵の値を前記第３のデータの値に書き換える処理を行うことを特徴とする請求項５記載のICカード。

【請求項７】前記演算処理手段は、

カード情報の送信を要求するコマンドデータを受信した時は、前記転送鍵識別子と、前記更新鍵識別子と、前記第１の公開鍵証明書を、レスポンスデータとして外部に送信する処理を行い、

前記転送鍵の更新許可を要求し、第２の公開鍵を含んだ第２の公開鍵証明書を格納しているコマンドデータを受信した時は、第１の乱数を生成して、前記第１の乱数をレスポンスデータとして外部に送信する処理を行い、

前記転送鍵の取得を要求し、第３の公開鍵を含んだ第３の公開鍵証明書と、第２の乱数を格納しているコマンドデータを受信した時は、まず、前記転送鍵識別子と、前記転送鍵を、公開鍵暗号方式に基づき、前記第３の公開鍵で暗号化した第１の暗号化データを作成し、次に、前記第１の暗号化データと、前記第２の乱数から、公開鍵暗号方式に基づき、前記秘密鍵で、第１のデジタル署名データを作成し、最後に、前記第１の暗号化データと、前記第１のデジタル署名データを、レスポンスデータとして外部に送信する処理を行い、

前記転送鍵の更新を要求し、第２の暗号化データと、第２のデジタル署名データを格納しているコマンドデータを受信した時は、まず、前記第２のデジタル署名データを、公開鍵暗号方式に基づき、前記第２の公開鍵で検証し、次に、前記第

２の暗号化データを、公開鍵暗号方式に基づき、前記秘密鍵で復号化して、第１のデータと、第２のデータを抽出し、最後に、前記第1のデータの値が、前記転送鍵識別子上限値と前記転送鍵の値との間に含まれるならば、前記転送鍵識別子の値を前記第1のデータの値に書き換えるとともに、前記転送鍵の値を前記第２のデータの値に書き換える処理を行うことを特徴とする請求項５記載のICカード。

【請求項８】外部と通信する通信手段と、データやプログラムを蓄積する情報蓄積手段と、情報処理を行う演算処理手段を有するICカードにおいて、

前記情報蓄積手段は、価値データと、前記価値データを更新するために使用する１個以上の転送鍵と、

現在選択している前記転送鍵を識別する選択転送鍵識別子と、前記転送鍵を更新するために使用する更新鍵を保存し、

前記演算処理手段は、前記更新鍵を用い、共通鍵暗号方式に基づいた暗号処理を行うことで、前記選択転送鍵識別子を更新する処理を行い、

その後、前記転送鍵を用い、共通鍵暗号方式に基づいた暗号処理を行うことで、前記価値データを更新する処理を行うことを特徴とするICカード。

【請求項９】前記演算処理手段において、

カード情報の送信を要求するコマンドデータを受信した時は、前記選択転送鍵識別子を、レスポンスデータとして外部に送信する処理を行い、

前記転送鍵の更新許可を要求するコマンドデータを受信した時は、第１の乱数を生成して、前記第１の乱数をレスポンスデータとして外部に送信する処理を行い、

前記転送鍵の取得を要求し、第２の乱数を格納しているコマンドデータを受信した時は、前記第２の乱数と、前記選択転送鍵識別子と、前記転送鍵を、共通鍵暗号方式に基づき、前記更新鍵で暗号化した、第１の暗号化データを、レスポンスデータとして外部に送信を行い、

前記転送鍵の更新を要求し、第２の暗号化データを格納しているコマンドデータを受信した時は、前記第２の暗号化データを、共通鍵暗号方式に基づき、前記更新鍵で復号化して、第１のデータと、第２のデータと、第３のデータを抽出し、

前記第１のデータが前記第１の乱数と等しく、且つ、前記第２のデータの値が、全ての前記転送鍵識別子のいずれかの値と等しいならば、前記選択転送鍵識別子の値を前記第２のデータの値に書き換える処理を行うことを特徴とする請求項８記載のICカード。

【請求項１０】第１の価値データを内部に保持している第1のICカードと通信する機能を有する第１のカード読書き手段と、第2の価値データを内部に保持している第2のICカードと通信する機能を有する第２のカード読書き手段と、前記第1のICカードと、前記第2のICカードとの間で、前記第１のICカードが保持している第1の転送鍵と、前記第2のICカードが保持している第2の転送鍵とを用いて、共通鍵暗号方式に基づいた暗号処理を行うことで、前記第１の価値データと前記第２の価値データの更新処理を行う演算処理手段を有する決済端末において、

前記演算処理手段は、

前記第1の転送鍵の新旧を値の大小で表す第１の転送鍵識別子を、前記第1のICカードから取得するとともに、前記第2の転送鍵の新旧を値の大小で表す第2の転送鍵識別子を、前記第２のICカードから取得し、

その後、前記第1の転送鍵識別子の値と前記第２の転送鍵識別子の値を比較し、値が異なっていたら、前記第１のICカードが保持している前記転送鍵の値と前記第2のICカードが保持している前記転送鍵の値のいずれかを、共通鍵暗号方式に基づいて更新する処理を行い、その後、共通鍵暗号方式に基づき前記価値データの更新処理を行うことを特徴とする決済端末。

【請求項１１】前記演算処理手段は、

前記第１のICカードから乱数を取得する処理を行い、

次に、前記乱数を前記第２のICカードに送信後、前記乱数と、前記第２の転送鍵識別子と、前記第２の転送鍵とを、共通鍵暗号化式に基づいて暗号化した、暗号化データを、前記第２のICカードから取得する処理を行い、

次に、前記暗号化データを、前記第１のICカードに送信することで、前記第1の転送鍵識別子の値を、前記第2の転送鍵識別子の値に更新するとともに、前記第1の転送鍵の値を、前記第2の転送鍵の値に更新する処理を行うことを特徴とする請求項10記載の決済端末。

【請求項１２】第１の価値データを内部に保持している第1のICカードと通信する機能を有する第１のカード読書き手段と、第2の価値データを内部に保持している第2のICカードと通信する機能を有する第２のカード読書き手段と、前記第1のICカードと、前記第2のICカードとの間で、前記第１のICカードが保持している第1の転送鍵と、前記第2のICカードが保持している第2の転送鍵とを用いて、共通鍵暗号方式に基づいた暗号処理を行うことで、前記第１の価値データと前記第２の価値データの更新処理を行う演算処理手段を有する決済端末において、

前記演算処理手段は、前記第1の転送鍵の新旧を値の大小で表す第１の転送鍵識別子と、第1の公開鍵証明書を、前記第１のICカードから取得するとともに、前記第2の転送鍵の新旧を値の大小で表す第2の転送鍵識別子と、第2の公開鍵証明書を、前記第2のICカードから取得する処理を行い、

その後、前記第1の転送鍵識別子の値と前記第２の転送鍵識別子の値を比較し、値が異なっていたら、前記第１のICカードが保持している前記転送鍵の値と前記第2のICカードが保持している前記転送鍵の値のいずれかを、公開鍵暗号方式に基づいて更新する処理を行い、その後、共通鍵暗号方式に基づき前記価値データの更新処理を行うことを特徴とする決済端末。

【請求項１３】前記演算処理手段は、

前記第１のICカードに前記第２の公開鍵証明書を送信した後に、前記第１のICカードから乱数を取得する処理を行い、

次に、前記第１の公開鍵証明書と、前記乱数を、前記第２のICカードに送信後、前記第２の転送鍵識別子と、前記第２の転送鍵とを、公開鍵暗号方式に基づき、暗号化した暗号化データと、前記乱数と、前記暗号化データとから、公開鍵暗号方式に基づいて作成したデジタル署名データとを、前記第２のICカードから取得する処理を行い、

次に、前記デジタル署名と、前記暗号化データを、前記第１のICカードに送信することで、前記第1の転送鍵識別子の値を、前記第2の転送鍵識別子の値に更新するとともに、前記第1の転送鍵の値を、前記第2の転送鍵の値に更新する処理を行うことを特徴とする請求項12記載の決済端末。

【請求項１４】第１の価値データを内部に保持している第1のICカードと通信す

る機能を有する第１のカード読書き手段と、第2の価値データを内部に保持している第2のICカードと通信する機能を有する第２のカード読書き手段と、前記第1のICカードと、前記第2のICカードとの間で、前記第１のICカードが保持している第1の転送鍵と、前記第2のICカードが保持している第2の転送鍵とを用いて、共通鍵暗号方式に基づいた暗号処理を行うことで、前記第１の価値データと前記第２の価値データの更新処理を行う演算処理手段を有する決済端末において、

前記演算処理手段は、

まず、前記第1の転送鍵の新旧を値の大小で表す第１の転送鍵識別子と、前記第1の転送鍵を更新するために用いる更新鍵の新旧を値の大小で表す第１の更新鍵識別子と、第１の公開鍵証明書を、前記第１のICカードから取得するとともに、前記第2の転送鍵の新旧を値の大小で表す第2の転送鍵識別子と、前記第２の転送鍵を更新するために用いる更新鍵の新旧を値の大小で表す第２の更新鍵識別子と、第２の公開鍵証明書を、前記第2のICカードから取得する処理を行い、

次に、前記第1の転送鍵識別子の値と前記第２の転送鍵識別子の値が異なっていて、且つ、前記第1の更新鍵識別子の値と前記第2の更新鍵識別子の値が等しければ、前記第１のICカードが保持している前記転送鍵の値と前記第2のICカードが保持している前記転送鍵の値のいずれかを、共通鍵暗号方式に基づいて更新する処理を行い、

前記第1の転送鍵識別子の値と前記第２の転送鍵識別子の値が異なっていて、且つ、前記第1の更新鍵識別子の値と前記第2の更新鍵識別子の値が異なっていれば、前記第１のICカードが保持している前記転送鍵の値と前記第2のICカードが保持している前記転送鍵の値のいずれかを、公開鍵暗号方式に基づいて更新する処理を行い、

その後、共通鍵暗号方式に基づいて前記価値データの更新処理を行う、演算処理手段を有することを特徴とする決済端末。

【請求項１５】前記演算処理手段は、

前記第2の転送鍵識別子の方が前記第1の転送鍵識別子より新しく、且つ、前記第１の更新鍵識別子の値と、前記第2の更新鍵識別子の値が等しければ、

まず、前記第１のICカードから乱数を取得する処理を行い、

次に、前記乱数を前記第２のICカードに送信後、前記乱数と、前記第２の転送鍵識別子と、前記第２の転送鍵とを、共通鍵暗号方式に基づいて暗号化した暗号化データを、前記第２のICカードから取得する処理を行い、

次に、前記暗号化データを前記第１のICカードに送信することで、前記第1の転送鍵識別子の値を、前記第2の転送鍵識別子の値に更新するとともに、前記第1の転送鍵の値を、前記第2の転送鍵の値に更新する処理を行うことを特徴とする請求項14記載の決済端末。

【請求項１６】前記演算処理手段は、

前記第2の転送鍵識別子の方が前記第1の転送鍵識別子より新しく、且つ、前記第１の更新鍵識別子の値と、前記第2の更新鍵識別子の値が異なっていれば、

まず、前記第１のICカードに前記第２の公開鍵証明書を送信した後に、前記第１のICカードから乱数を取得する処理を行い、

次に、前記第１の公開鍵証明書と、前記乱数を、前記第２のICカードに送信後、前記第２の転送鍵識別子と、前記第２の転送鍵とを、公開鍵暗号方式に基づき、暗号化した暗号化データと、前記乱数と、前記暗号化データとから、公開鍵暗号方式に基づいて作成したデジタル署名データとを、前記第２のICカードから取得する処理を行い、

次に、前記デジタル署名と、前記暗号化データを、前記第１のICカードに送信することで、前記第1の転送鍵識別子の値を、前記第2の転送鍵識別子の値に更新するとともに、前記第1の転送鍵の値を、前記第2の転送鍵の値に更新する処理を行うことを特徴とする請求項14記載の決済端末。

【請求項１７】

他のICカードと価値データを送受信するICカードであって、

該価値データと、該価値データを更新するために用いる転送鍵と、該転送鍵を更新するために用いる更新鍵と、を蓄積する情報蓄積手段と、

該他のICカードから送信された、該更新鍵を用いて暗号化された転送鍵を受信する通信手段と、

該暗号化された転送鍵を該更新鍵を用いて復号化し、該復号化した転送鍵により該情報蓄積手段に蓄積されている転送鍵を更新する演算処理手段と、

を備えることを特徴とするICカード。

【請求項１８】

他のICカードと価値データを送受信するICカードであって、

該価値データと、該価値データを更新するために用いる転送鍵と、該転送鍵を更新するために用いる公開鍵暗号方式の秘密鍵と、を蓄積する情報蓄積手段と、

該他のICカードから送信された、該秘密鍵に対応する公開鍵を用いて暗号化された転送鍵を受信する通信手段と、

該暗号化された転送鍵を該秘密鍵を用いて復号化し、該復号化した転送鍵により該情報蓄積手段に蓄積されている転送鍵を更新する演算処理手段と、

を備えることを特徴とするICカード。

【請求項１９】

第１の価値データ、該第１の価値データを更新するために用いる第１の転送鍵、及び該第１の転送鍵を更新するために用いる更新鍵を蓄積している第１のICカードと、第２の価値データ、該第２の価値データを更新するために用いる第２の転送鍵、及び該第２の転送鍵を更新するために用いる更新鍵を蓄積している第２のICカードと、の間で該価値データを送受信する決済端末であって、

該第１の転送鍵と該第２の転送鍵とが異なる場合に、該更新鍵で暗号化された該第１の転送鍵を該第１のICカードから受信する第１のカード読み書き手段と、

該更新鍵で暗号化された該第１の転送鍵を含む、該第２のICカードの該第２の転送鍵を該第１の転送鍵に更新することを要求する転送鍵更新要求を該第２のICカードに送信する第２のカード読み書き手段と、

を備えることを特徴とする決済端末。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子マネーやポイントを扱う、ICカードおよび決済端末に関する。

【０００２】

【従来の技術】

近年ICカードが磁気カードに代わって広く普及しつつある。これはICカードに

は、記憶容量が大きい、暗号処理などを行うための演算装置を備えている、容易に内部を観察できない（耐タンパ性を有している）、といった磁気カードにはない特徴があるからである。このような特徴を持ったICカードを、決済システムに適用することで、磁気カードに比べてセキュリティを向上させたり、磁気カードでは実現できなかった新しいサービスを提供したりできる。

【０００３】

【発明が解決しようとする課題】

ICカードを用いたサービスとして例えば、電子マネーやポイントといった価値のある値である「バリュー」をICカード内に格納しておき、このバリューをICカード間で転送することで、各種決済を行うことが考えられる。このような決済処理を行うためには、バリューの不正な複製や改ざんを防止できなければならない。このためには、ICカードの特徴である耐タンパ性と、暗号処理を行いたICカード間の通信処理が必要となる。

【０００４】

ここで、暗号処理の方式は、公開鍵暗号方式と共通鍵暗号方式とに大別される。公開鍵方式は、通信を行う両者の間で暗号鍵を共有していなくても、暗号通信が行えるという利点があるが、一般に共通鍵暗号方式に比べて処理速度が遅い。一方で共通鍵暗号方式は、高速な暗号処理を実現できるが、予め暗号通信を行う両者の間で暗号鍵を共有しておく必要がある。

【０００５】

ICカード間でバリューを転送するために必要な時間は、できるだけ短い方が、使い勝手が良くなるのは明らかである。したがって、バリュー転送時に用いる暗号方式として、処理速度の速い共通鍵暗号方式を選択した方が、使い勝手は向上する。しかし、共通鍵暗号方式を用いた場合、全てのICカードに同一の暗号鍵を設定しておく必要がある。このため、バリュー転送に使用する暗号鍵を更新する時は、バリュー転送できないカードの組み合わせが生じないように、全てのICカードの暗号鍵を同時に更新する必要があるといった課題がある。

【０００６】

そこで、本発明は、ICカード間のバリュー転送に共通鍵暗号方式を用いた場合

に、バリュー転送で使用する暗号鍵を容易に更新可能にすることで、システム全体のセキュリティを向上できるICカードおよび決済端末を提供することを目的とする。

【０００７】

【課題を解決するための手段】

上記目的を達成するために本発明のICカードは、他のICカードと価値データを送受信するICカードであって、該価値データと、該価値データを更新するために用いる転送鍵と、該転送鍵を更新するために用いる更新鍵と、を蓄積する情報蓄積手段と、該他のICカードから送信された、該更新鍵を用いて暗号化された転送鍵を受信する通信手段と、該暗号化された転送鍵を該更新鍵を用いて復号化し、該復号化した転送鍵により該情報蓄積手段に蓄積されている転送鍵を更新する演算処理手段と、を備えることを特徴とする。

【０００８】

また、上記目的を達成するために本発明の決済端末は、第１の価値データ、該第１の価値データを更新するために用いる第１の転送鍵、及び該第１の転送鍵を更新するために用いる更新鍵を蓄積している第１のICカードと、第２の価値データ、該第２の価値データを更新するために用いる第２の転送鍵、及び該第２の転送鍵を更新するために用いる更新鍵を蓄積している第２のICカードと、の間で該価値データを送受信する決済端末であって、該第１の転送鍵と該第２の転送鍵とが異なる場合に、該更新鍵で暗号化された該第１の転送鍵を該第１のICカードから受信する第１のカード読み書き手段と、該更新鍵で暗号化された該第１の転送鍵を含む、該第２のICカードの該第２の転送鍵を該第１の転送鍵に更新することを要求する転送鍵更新要求を該第２のICカードに送信する第２のカード読み書き手段と、を備えることを特徴とする。

【０００９】

【発明の実施の形態】

以下、本発明の実施形態について説明していく。

まず、第１の実施形態について説明する。図１に、本実施形態に係わるバリュー転送システムの構成要素ブロック図を示す。図１において、100Aと100BはICカ

ード、110は決済端末である。決済端末110は、ICカード100AとICカード100Bの間でバリュー転送を行うために用い、例えばPDAといった携帯端末や、POSなどの店舗端末、あるいは、ATMなどの金融端末などが考えられる。

【００１０】

次に、ICカード100Aの内部構成について説明する。なお、ICカード100Bの内部構成はICカード100Aと同様であるため説明は省略する。ICカード100Aは、通信手段201Aと、情報蓄積手段202Aと、演算制御手段203Aを含んだ構成となっている。ここで、通信手段201Aは、決済端末110と通信を行い、決済端末110からコマンドを受信したり、決済端末110にレスポンスを返信したりする機能を有する。情報蓄積手段202Aは、ICカードが提供するサービスを実行するプログラムやデータ、あるいは決済端末110から取得した情報等を一時的あるいは永続的に格納する機能を有し、ROM(Read Only Memory)、RAM(Random Access Memory)、フラッシュメモリ等の半導体メモリから構成される。演算制御手段203Aは、マイクロプロセッサを用いることで、ICカード全体の制御を司り、情報蓄積手段202Aに格納されているプログラムを実行する機能を有する。また、暗号処理を高速化するための専用ハードウェア回路を含んでいても良い。

【００１１】

次に、情報蓄積手段202Aに含まれるデータおよびプログラムについて説明する。情報蓄積手段202Aは、有効期限111Aと、バリュー残高108Aと、鍵情報204Aと、決済プログラム205Aを含んだ構成になっている。有効期限111Aは、ICカード100Aの有効期限を表すデータである。バリュー残高108AはICカード100Aが保持しているバリューの残高を表す。鍵情報204Aは、バリュー転送を行うために使用する鍵データを含んでいる。決済プログラム205Aは、鍵更新およびバリュー転送を行うプログラムであり、演算処理手段203Aにより実行される。

【００１２】

ここで、ICカードはその通信方式により、接触型と非接触型に分類される。それぞれの仕様はすでに標準化されており、例えば、接触型ICカードは、ISO(International Organization for Standardization: 国際標準化機構)で、ISO/IEC7816として標準化されている。また、非接触型ICカードは、ISO/IEC14443で標準化

されている。ISO/IEC7816およびISO/IEC14443に基づくICカードは、端末から送信するコマンドに従って内部で演算を行い、結果をレスポンスとして返すということを順次行っていくことで、サービスを実現するための処理を遂行していく。ここで、ICカード-端末間で送受信するコマンドとレスポンスは、APDU(Application Protocol Data Unit)という形式での定義が、ISO/IEC7816でなされている。本発明においては、通信手段201Aは接触型と非接触型のどちらの方式であっても適用範囲である。

【００１３】

次に、決済端末110の内部構成について説明する。携帯端末110は、カード読書き手段301Aおよび301Bと、情報蓄積手段302と、演算制御手段303と、操作手段304を含んだ構成となっている。カード読書き手段301Aは、ICカード100Aと通信するために、ICカード100Aにコマンドを送信したり、ICカードからレスポンスを受信したりする機能を有する。同様に、カード読書き手段301Bは、ICカード100Bと通信する機能を有する。ここで、カード読書き手段301Aとカード読書き手段301Bは、接触型であっても非接触型であっても、本発明の適用範囲である。情報蓄積手段302は、プログラムやデータなどを一時的あるいは永続的に蓄積する機能を有し、例えばハードディスクや半導体メモリ等から構成される。演算処理手段303は、マイクロプロセッサを用いて、情報蓄積手段302に格納されているプログラムに基づいて、決済端末110全体を制御し、決済処理を遂行する機能を有する。操作手段304は、決済端末110を操作する人に対して、決済端末110を操作するためのインターフェイスを提供し、例えば、キーボード、バーコードリーダ、ディスプレイ等から構成される。また、情報蓄積手段302には、決済プログラム305が格納されている。決済プログラム305は、ICカード100AとICカード100Bの間で、鍵の更新処理およびバリュー転送処理を行うためのプログラムであり、演算処理手段303により実行される。

【００１４】

次に、鍵情報204Aのデータ構成図を図２に示す。図２において、鍵情報204Aは、更新鍵105Aと、転送鍵ID106Aと、転送鍵107Aと、転送鍵ID上限値112Aとったデータを格納している。なお、ICカード100Bも同様のデータ構成となっている。こ

こで、更新鍵105Aは転送鍵107Aを更新するために用いる共通鍵暗号方式の鍵データであり、転送鍵107Aの暗号化および復号化を行う時に用いる。また、転送鍵ID 106Aは転送鍵107Aを一意に識別するための番号であり、転送鍵の新旧を値の大小で判別する。例えば、転送鍵IDの値が大きいほど新しい転送鍵と見なす。あるいは他の方法で転送鍵の新旧を判別しても本発明の適用範囲である。また、転送鍵107Aは、バリューを転送するために用いる共通鍵暗号方式の鍵データである。転送鍵ID上限値 112Aは、ICカード100Aに格納可能な転送鍵ID106Aの値の上限値を表すデータである。ここで、更新鍵105A、および転送鍵107Aを用いる暗号アルゴリズムは、共通鍵暗号方式であれば、どのようなアルゴリズムを用いても本発明の適用範囲である。なお、更新鍵105Aと転送鍵107AはICカード100A外部からの読み出しが行えないものとする。

【００１５】

次に、決済端末110を用いて、ICカード100AとICカード100Bの間で、転送鍵を更新するための処理を詳細に説明していく。この処理は、バリュー転送を行う前に実行する。また、決済端末110がICカード100AおよびICカード100Bに送信するコマンドはAPDU形式を用いるものとして説明していく。また、ICカード100Aの更新鍵105Aの値と、ICカード100Bの更新鍵105Bの値は等しいものとする。

【００１６】

図３は、転送鍵を更新するための処理フロー図である。まず、決済端末110は、処理S1001として、ICカード100AおよびICカード100Bに格納されている、決済サービスプログラムを選択起動するために、決済サービス選択要求をAPDUコマンドで送信する。

【００１７】

次に、決済端末110は、処理S1002として、ICカード100AおよびICカード100Bにカード情報取得要求をAPDUコマンドで送信する。ICカード100Aは、カード情報取得要求を受信すると、処理S1101Aとして、転送鍵ID 106Aと有効期限111Aを、決済端末110にAPDUレスポンスで送信する。同様に、ICカード100Bは、カード情報取得要求を受信すると、処理S1101Bとして、転送鍵ID 106Bと有効期限111Bを決済端末110にAPDUレスポンスで送信する。

【００１８】

次に、決済端末110は、処理S1003として転送鍵更新チェックを行う。この処理では、まず、受信した有効期限111Aと有効期限111Bとを調べ、いずれも現在の日付より未来であることを確認する。もし、いずれかが、現在の日付より過去であれば、転送鍵更新処理を中止する。次に、決済端末110は、受信した転送鍵ID 106Aと転送鍵ID 106Aとを比較し、転送鍵を更新する必要があるかどうかを判定する。もし、転送鍵ID 106Aが転送鍵ID 106Bより新しい場合は、ICカード100Bの転送鍵ID 106Bと転送鍵107Bを、ICカード100Aの転送鍵ID 106Aと転送鍵107Aに更新する処理を以下行っていく。あるいはもし、転送鍵ID 106Bが転送鍵ID 106Aより新しい場合は、ICカード100Aの転送鍵ID 106Aと転送鍵107Aを、ICカード100Bの転送鍵ID 106Bと転送鍵107Bに更新する処理を以下行っていく。あるいはもし、転送鍵ID 106Aと転送鍵ID 106Bが同一の場合は、以降の転送鍵更新処理を行わずに、直ちにバリュー転送処理に移行する。図３は転送鍵ID 106Bが転送鍵ID 106Aより新しかった場合の処理フローとなっており、以下この場合について説明を行っていく。

【００１９】

次に、決済端末110は、処理S1004として、ICカード100Aに、転送鍵更新許可要求をAPDUコマンドで送信する。ICカード100Aは、転送鍵更新許可要求を受信すると、処理S1102Aとして、更新乱数1121を生成し、これをAPDUレスポンスで、決済端末110に送信する。ここで、更新乱数1121は、不正なカードによってICカード100Aの転送鍵107Aが不正に書き換えられないように、動的認証を行うために用いる。また、更新乱数1121の乱数生成アルゴリズムは、本発明では特に規定しない。

【００２０】

次に、決済端末110は、処理S1005として、ICカード100Bに、転送鍵取得要求を、APDUコマンドで送信する。このAPDUコマンドには、更新乱数1121が含まれている。ICカード100Bは、転送鍵取得要求として、更新乱数1121を受信すると、処理S1102Bとして、更新乱数1121と、転送鍵ID 106Bと、転送鍵107Bを、更新鍵105Bで暗号化し、これをAPDUレスポンスで、決済端末110に送信する。

【００２１】

次に、決済端末は、処理S1006として、ICカード100Aに、転送鍵更新要求をAPDUコマンドで送信する。このAPDUコマンドには、更新乱数1121と、転送鍵ID 106Bと、転送鍵107Bを、更新鍵105Bで暗号化したデータが含まれている。ICカード100Aは、転送鍵更新要求として、更新乱数1121と、転送鍵ID 106Bと、転送鍵107Bを、更新鍵105Bで暗号化したデータを受信すると、処理S1103Aとして、更新鍵105Aで復号化し、復号された更新乱数1121が正しい値かどうかを確認する。もし、正しくない値であったなら、動的認証が失敗したと見なし、転送鍵更新処理を中止する。もし、正しい値であったなら、動的認証が成功したと見なし、処理S1104Aを行う。この処理では、まず、転送鍵ID106Bの値が、転送鍵ID上限値112Aと転送鍵ID106Aの値との間に含まれていることを確認する。もし確認が失敗したら転送鍵の更新は行わない。もし確認が成功したら、転送鍵ID 106Aの値と転送鍵107Aの値を、転送鍵ID 106Bの値と、転送鍵107Bの値に書き換える。

【００２２】

以上説明した手順において、処理S1001と、処理S1002と、処理S1003と、処理S1004と、処理S1005と、処理S1006は、決済端末110の演算制御手段303で実行する決済プログラム305により処理される。また、処理S1101Aと、処理S1102Aと、処理S1103Aと、処理S1104Aは、ICカード100Aの演算制御手段203Aで実行する決済プログラム205Aにより処理される。また、処理S1101Bと、処理S1102Bと、処理S1103Bと、処理S1104Bは、ICカード100Bの演算制御手段203Bで実行する決済プログラム205Bにより処理される。

【００２３】

以上の手順により、転送鍵をより新しい値に、安全に書き換えることができる。また、転送鍵の更新は、共通鍵暗号方式を使って行うため、短時間で処理を完了することが可能である。さらに、更新可能である転送鍵の範囲を、更新鍵ID上限値を用いて制限することが可能になる。

【００２４】

次に、決済端末110を用いて、ICカード100AとICカード100Bの間で、バリューを転送するための処理を詳細に説明していく。この処理は、図３で説明した転送

鍵更新処理の後に行い、転送鍵107Aの値と転送鍵107Bの値は等しいものとする。また、決済端末110がICカード100AおよびICカード100Bに送信するコマンドはAPDU形式を用いるものとして説明していく。図４は、バリューを転送するための処理フロー図である。まず、決済端末110は、処理S2001として、ICカード100Aに、バリュー送信許可要求として、APDUコマンドを送信する。このAPDUコマンドには、支払いバリュー221と取引日付222が含まれている。ここで、支払いバリュー221は、転送するバリューの値を表している。また取引日付222は、バリュー転送を行う日時を表す。ICカード100Aは、バリュー送信許可要求として、支払いバリュー221と取引日付222を取得すると、処理S2101として、バリュー残高仮更新を行う。すなわち、バリュー残高108Aの値から支払いバリュー221を減算した値を、仮のバリュー残高の値としておく。そして、処理S2102Aとして、送信乱数223を生成し、これをAPDUレスポンスで、決済端末110に送信する。ここで、送信乱数223は、不正なカードによってICカード100Aのバリュー残高108Aを書き換えられないように、動的認証を行うために用いる。また、送信乱数223の乱数生成アルゴリズムは、本発明では特に規定しない。

【００２５】

次に、決済端末110は、処理S2002として、ICカード100Bに、バリュー受信許可要求を、APDUコマンドで送信する。このAPDUコマンドには、支払いバリュー221と取引日付222と、送信乱数223が含まれている。ICカード100Bは、バリュー受信許可要求として、支払いバリュー221と取引日付222と、送信乱数223を受信すると、処理S2101Bとして、バリュー残高仮更新を行う。すなわち、バリュー残高108Bの値と支払いバリュー221を加算した値を、仮のバリュー残高の値としておく。そして、処理S2102Bとして、送信チャレンジ224を作成する。ここで、送信チャレンジ224は、支払いバリュー221と、取引日付222と、送信乱数223を結合したデータを、転送鍵107Bを用いて暗号処理を行った結果得られる認証コードである。本発明においては転送鍵を用いて認証コードを生成するアルゴリズムは特に規定しない。例えば、ISO9797にて規定されているアルゴリズムを用いることが考えられる。その後、ICカード100Bは、処理S2103Bとして、受信乱数225を生成しする。そして、送信チャレンジ224と受信乱数225を、APDUレスポンスで、決済端

末110に送信する。ここで、送信乱数225は、不正なカードによってICカード100Bのバリュー残高108Bを書き換えられないように、動的認証を行うために用いる。また、送信乱数225の乱数生成アルゴリズムは、本発明では特に規定しない。

【００２６】

次に、決済端末110は、処理S2003として、ICカード100Aに、バリュー送信要求を、APDUコマンドとして送信する。このAPDUコマンドには、送信チャレンジ224と受信乱数225が含まれている。ICカード100Aは、送信チャレンジ224と受信乱数225を受信すると、まず、処理2103Aとして、送信チャレンジ224の検証を行う。すなわち、支払いバリュー221と、取引日付222と、送信乱数223を結合したデータを、転送鍵107Aを用いて暗号処理を行った結果得られる認証コードと、送信チャレンジ224が等しいかどうかと確認する。もし、等しくなかったなら、動的認証が失敗したと見なし、バリュー転送処理を中止する。もし、等しかったなら、動的認証が成功したと見なし、続いて、処理S2104Aとして、バリュー残高更新を行う。すなわち、バリュー残高108Aの値から、支払いバリュー221を減算し、これでバリュー残高108Aの値を書き換える。その後、処理S2105Aとして、受信チャレンジ226を作成し、これをAPDUレスポンスとして、決済端末110に送信する。ここで、送信チャレンジ226は、支払いバリュー221と、取引日付222と、受信乱数225を結合したデータを、転送鍵107Aを用いて暗号処理を行った結果得られる認証コードである。

【００２７】

次に、決済端末110は、処理S2004として、ICカード100Bに、バリュー受信要求を、APDUコマンドとして送信する。このAPDUコマンドには、受信チャレンジ226が含まれている。ICカード100Bは、受信チャレンジ226を受信すると、まず、処理2104Bとして、受信チャレンジ226の検証を行う。すなわち、支払いバリュー221と、取引日付222と、受信乱数225を結合したデータを、転送鍵107Bを用いて暗号処理を行った結果得られる認証コードと、受信チャレンジ226が等しいかどうかと確認する。もし、等しくなかったなら、動的認証が失敗したと見なし、バリュー転送処理を中止する。もし、等しかったなら、動的認証が成功したと見なし、続いて、処理S2105Bとして、バリュー残高更新を行う。すなわち、バリュー残

高108Bの値に、支払いバリュー221を加算し、これでバリュー残高108Bの値を書き換える。その後、APDUレスポンスを、決済端末110に送信する。

【００２８】

以上説明した手順において、処理S2001と、処理S2002と、処理S2003と、処理S2004は、決済端末110の演算制御手段303で実行する決済プログラム305により処理される。また、処理S2101Aと、処理S2102Aと、処理S2103Aと、処理S2104Aと、処理S2105Aは、ICカード100Aの演算制御手段203Aで実行する決済プログラム205Aにより処理される。また、処理S2101Bと、処理S2102Bと、処理S2103Bと、処理S2104Bと、処理S2105Bは、ICカード100Bの演算制御手段203Bで実行する決済プログラム205Bにより処理される。

【００２９】

以上の手順により、ICカード100AとICカード100Bとの間で、バリュー転送を安全に行うことが可能になる。なお、図４を用いて説明したバリューを転送するための処理手順と異なっていても、共通の転送鍵を用いてバリューを転送する方式ならば、本発明の適用範囲となる。

【００３０】

以上、説明を行ってきた、本発明に係わる第1の実施例においては、ICカード100AとICカード100Bとの間で、転送鍵が異なっていても、更新鍵を用いて、両カード内の転送鍵の値を、新しい値に更新することが可能になる。例えば、有効期限が切れたICカードを、新しいICカードに切替える時に、転送鍵も新しい値に、更新しておけば、この新しいICカードとバリュー転送を行った、古いICカードの転送鍵の値を、新しい値に更新することができ、セキュリティを向上することが可能になる。

【００３１】

次に、本発明に係わる第2の実施例について説明する。本実施例においては、転送鍵の更新を、公開鍵暗号方式を用いて行う。図５は、本実施例におけるバリュー転送システムの構成要素ブロック図であるが、これは、第1の実施例で説明した図1のブロック図と同じ構成となっている。次に、ICカード100Aの鍵情報204Aの詳細について説明する。

【００３２】

図６は鍵情報204Aのデータ構成図である。図６において、鍵情報204Aは、CA公開鍵101と、カード公開鍵証明書102Aと、カード秘密鍵103Aと、転送鍵ID 106Aと、転送鍵107Aと、転送鍵ID上限値112Aを含んでいる。また、ICカード100Bの鍵情報204Ｂも同様のデータ構成となる。ここで、CA公開鍵101は、任意の認証局の公開鍵であり、カード公開鍵証明書102Aを検証するために用いる。カード公開鍵証明書102Aは、カード秘密鍵103Aと対の鍵データであるカード公開鍵の正当性を証明するためのデータであり、このカード公開鍵はカード公開鍵証明書102Aの内部に含まれている構成となっている。カード秘密鍵103Aは、公開鍵暗号方式の秘密鍵であり、転送鍵を更新するために用いる。

【００３３】

また、転送鍵ID 106Aは転送鍵107Aを一意に識別するための番号であり、転送鍵の新旧を値の大小で判別する。例えば、転送鍵IDの値が大きいほど新しい転送鍵と見なす。また、転送鍵107Aは、バリューを転送するために用いる共通鍵暗号方式の鍵データである。転送鍵ID上限値 112Aは、ICカード100Aに格納可能な転送鍵ID106Aの値の上限値を表すデータである。なお、CA公開鍵101、カード公開鍵証明書102A、カード秘密鍵103Aを用いる暗号アルゴリズムは、公開鍵暗号方式であれば、どのようなアルゴリズムを用いても本発明の適用範囲である。また、カード秘密鍵103Aと、転送鍵107Aは、ICカード100A外部からの読出しが行えないものとする。

【００３４】

次に、本実施例に係わる、転送鍵を更新するための処理を詳細に説明していく。この処理は、バリュー転送を行う前に実行する。また、決済端末110がICカード100AおよびICカード100Bに送信するコマンドはAPDU形式を用いるものとして説明していく。図７は、転送鍵を更新するための処理フロー図である。まず、決済端末110は、処理S3001として、ICカード100AおよびICカード100Bに格納されている、決済サービスプログラムを選択起動するために、決済サービス選択要求をAPDUコマンドで送信する。

【００３５】

次に、決済端末110は、処理S3002として、ICカード100AおよびICカード100Bにカード情報取得要求をAPDUコマンドで送信する。ICカード100Aは、カード情報取得要求を受信すると、処理S3101Aとして、カード公開鍵証明書102Aと、転送鍵ID 106Aと有効期限111Aを、決済端末110にAPDUレスポンスで送信する。同様に、ICカード100Bは、カード情報取得要求を受信すると、処理S3101Bとして、カード公開鍵証明書102Bと、転送鍵ID 106Bと有効期限111Bを決済端末110にAPDUレスポンスで送信する。

【００３６】

次に、決済端末110は、処理S3003として転送鍵更新チェックを行う。この処理では、まず、受信した有効期限111Aと有効期限111Bとを調べ、いずれも現在の日付より未来であることを確認する。もし、いずれかが、現在の日付より過去であれば、転送鍵更新処理を中止する。次に、決済端末110は、受信した転送鍵ID 106Aと転送鍵ID 106Bとを比較し、転送鍵を更新する必要があるかどうかを判定する。もし、転送鍵ID 106Aが転送鍵ID 106Bより新しい場合は、ICカード100Bの転送鍵ID 106Bと転送鍵107Bを、ICカード100Aの転送鍵ID 106Aと転送鍵107Aに更新する処理を以下行っていく。あるいはもし、転送鍵ID 106Bが転送鍵ID 106Aより新しい場合は、ICカード100Aの転送鍵ID 106Aと転送鍵107Aを、ICカード100Bの転送鍵ID 106Bと転送鍵107Bに更新する処理を以下行っていく。あるいはもし、転送鍵ID 106Aと転送鍵ID 106Bが同一の場合は、以降の転送鍵更新処理を行わずに、直ちにバリュー転送処理に移行する。図７は転送鍵ID 106Bが転送鍵ID 106Aより新しかった場合の処理フローとなっており、以下この場合について説明を行っていく。

【００３７】

次に、決済端末110は、処理S3004として、ICカード100Aに、転送鍵更新許可要求をAPDUコマンドで送信する。このAPDUコマンドには、カード公開鍵証明書102Bが含まれている。ICカード100Aは、転送鍵更新許可要求として、カード公開鍵証明書102Bを受信すると、処理S3102Aとして、更新カード公開鍵証明書102BをCA公開鍵101で検証し、検証が成功したら、更新乱数3121を生成する。そして、更新乱数3121をAPDUレスポンスで、決済端末110に送信する。ここで、更新乱数3121

は、不正なカードによってICカード100Aの転送鍵107Aが不正に書き換えられないように、動的認証を行うために用いる。また、更新乱数3121の乱数生成アルゴリズムは、本発明では特に規定しない。

【００３８】

次に、決済端末110は、処理S3005として、ICカード100Bに、転送鍵取得要求を、APDUコマンドで送信する。このAPDUコマンドには、カード公開鍵証明書102Aと、更新乱数3121が含まれている。ICカード100Bは、転送鍵取得要求として、カード公開鍵証明書102Aと、更新乱数3121を受信すると、処理S3102Bとして、まず、カード公開鍵証明書102Aを、CA公開鍵101で検証する。検証が成功したら、転送鍵ID 106Bと転送鍵107Bを、カード公開鍵証明書102Aに含まれるカード公開鍵で暗号化する。次に、処理S3103Bとして、カード秘密鍵103Bを用いて、転送鍵ID 106Bと転送鍵107Bを暗号化したデータと、更新乱数3121とに対するデジタル署名3122を生成する。そして、転送鍵ID 106Bと転送鍵107Bを暗号化したデータと、デジタル署名3122を、APDUレスポンスで、決済端末110に送信する。ここで、デジタル署名3122の作成アルゴリズムは、公開鍵暗号方式に基づいたものであれば、どのようなアルゴリズムでも本発明の適用範囲である。

【００３９】

次に、決済端末は、処理S3006として、ICカード100Aに、転送鍵更新要求をAPDUコマンドで送信する。このAPDUコマンドには、デジタル署名3122と、転送鍵ID 106Bと転送鍵107Bを暗号化したデータとが含まれている。ICカード100Aは、転送鍵更新要求として、デジタル署名3122と、転送鍵ID 106Bと転送鍵107Bを暗号化したデータを受信すると、まず、処理S3103Aとして、カード公開鍵102Bを用いて、デジタル署名3122の検証を行う。この検証が成功したら、動的認証が成功したと見なし、次に、処理S3104Aとして、転送鍵ID 106Bと転送鍵107Bを、カード秘密鍵103Aで復号化する。そして、処理S3105Aを行う。この処理では、転送鍵ID106Bの値が、転送鍵ID上限値112Aと転送鍵ID106Aの値との間に含まれていることを確認するもし確認が失敗したら転送鍵の更新は行わない。もし確認が成功したら、転送鍵ID 106Aの値と転送鍵107Aの値を、転送鍵ID 106Bの値と転送鍵107Bの値に書き換える。

【００４０】

以上説明した手順において、処理S3001と、処理S3002と、処理S3003と、処理S3004と、処理S3005と、処理S3006は、決済端末110の演算制御手段303で実行する決済プログラム305により処理される。また、処理S3101Aと、処理S3102Aと、処理S3103Aと、処理S3104Aと、処理S3105Aは、ICカード100Aの演算制御手段203Aで実行する決済プログラム205Aにより処理される。また、処理S3101Bと、処理S3102Bと、処理S3103Bは、ICカード100Bの演算制御手段203Bで実行する決済プログラム205Bにより処理される。

【００４１】

以上の手順により、転送鍵をより新しい値に、安全に書き換えることができる。本発明に係わる第2の実施例においては、ICカード100AとICカード100Bとの間で、転送鍵が異なっていても、カード公開鍵およびカード秘密鍵を用いて、両カード内の転送鍵の値を、新しい値に更新することが可能になる。例えば、有効期限が切れたICカードを、新しいICカードに切替える時に、転送鍵も新しい値に更新しておけば、この新しいICカードとバリュー転送を行った、古いICカードの転送鍵の値を、新しい値に更新することができ、セキュリティを向上することが可能になる。

【００４２】

また、本実施例においては、CA公開鍵および公開鍵証明書を用いるため、CRL(Certificate Revocation List)を用いて、無効となった公開鍵証明書を保持しているICカードとはバリュー転送を行わないようにすることも可能である。ここで、CRLは無効になった証明書のシリアル番号の一覧に、認証局(CA)が電子署名をしたデータであり、例えば、決済端末110がCRLを保持していて、ICカード100Aから取得したカード公開鍵証明書102Aと、ICカード100Bから取得したカード公開鍵証明書102Bのチェックを、CRLを用いて行う場合も、本発明の適用範囲である。また、決済端末110は、CRLをネットワーク経由で認証局から取得してもよい。あるいは、決済端末110の製造時に最新のCRLを内蔵しておいてもよい。

【００４３】

次に、本発明に係わる第3の実施例について説明する。本実施例においては、

転送鍵の更新に、共通鍵暗号方式と公開鍵暗号方式のどちらを用いるかを選択できるようになっている。図８は、本実施例におけるバリュー転送システムの構成要素ブロック図であるが、これは、第1の実施例で説明した図1のブロック図と同じ構成となっている。次に、ICカード100Aの鍵情報204Aの詳細について説明する。

【００４４】

図９は鍵情報204Aのデータ構成図である。図９において、鍵情報204Aは、CA公開鍵101と、カード公開鍵証明書102Aと、カード秘密鍵103Aと、更新鍵ID 104Aと、更新鍵105Aと、転送鍵ID 106Aと、転送鍵107Aと、転送鍵ID上限値112Aを含んでいる。また、ICカード100Bも同様のデータ構成となる。ここで、CA公開鍵101は、任意の認証局の公開鍵であり、カード公開鍵証明書102Aを検証するために用いる。カード公開鍵証明書102Aは、カード秘密鍵103Aと対の鍵データであるカード公開鍵の正当性を証明するためのデータであり、このカード公開鍵はカード公開鍵証明書102Aの内部に含まれている構成となっている。カード秘密鍵103Aは、公開鍵暗号方式の秘密鍵であり、転送鍵を更新するために用いる。また、更新鍵ID104Aは、更新鍵105Aを一意に識別するための番号であり、更新鍵の新旧を値の大小で判別する。例えば、更新鍵IDの値が大きいほど新しい更新鍵と見なす。更新鍵105Aは転送鍵107Aを更新するために用いる共通鍵暗号方式の鍵データであり、転送鍵107Aの暗号化および復号化を行う時に用いる。また、転送鍵ID 106Aは転送鍵107Aを一意に識別するための番号であり、転送鍵の新旧を値の大小で判別する。例えば、転送鍵IDの値が大きいほど新しい転送鍵と見なす。また、転送鍵107Aは、バリューを転送するために用いる共通鍵暗号方式の鍵データである。転送鍵ID上限値 112Aは、ICカード100Aに格納可能な転送鍵ID106Aの値の上限値を表すデータでる。なお、更新鍵105A、および転送鍵107Aを用いる暗号アルゴリズムは、共通鍵暗号方式であれば、どのようなアルゴリズムを用いても本発明の適用範囲である。また、CA公開鍵101、カード公開鍵証明書102A、カード秘密鍵103Aを用いる暗号アルゴリズムは、公開鍵暗号方式であれば、どのようなアルゴリズムを用いても本発明の適用範囲である。また、カード秘密鍵103Aと、更新鍵104Aと、転送鍵107Aは、ICカード100A外部からの読出しが行えないものとする。

【００４５】

次に、本実施例に係わる、転送鍵を更新するための処理を詳細に説明していく。この処理は、バリュー転送を行う前に実行する。また、決済端末110がICカード100AおよびICカード100Bに送信するコマンドはAPDU形式を用いるものとして説明していく。図１０は、転送鍵を更新するための処理フロー図である。まず、決済端末110は、処理S4001として、ICカード100AおよびICカード100Bに格納されている、決済サービスプログラムを選択起動するために、決済サービス選択要求をAPDUコマンドで送信する。

【００４６】

次に、決済端末110は、処理S4002として、ICカード100AおよびICカード100Bにカード情報取得要求をAPDUコマンドで送信する。ICカード100Aは、カード情報取得要求を受信すると、処理S4101Aとして、カード公開鍵証明書102Aと更新鍵ID 104Aと転送鍵ID 106Aと有効期限111Aを、決済端末110にAPDUレスポンスで送信する。同様に、ICカード100Bは、カード情報取得要求を受信すると、処理S4101Bとして、カード公開鍵証明書102Bと更新鍵ID 104Bと転送鍵ID 106Bと有効期限111Bを決済端末110にAPDUレスポンスで送信する。

【００４７】

次に、決済端末110は、処理S4003として転送鍵更新チェックを行う。この処理では、まず、受信した有効期限111Aと有効期限111Bとを調べ、いずれも現在の日付より未来であることを確認する。もし、いずれかが、現在の日付より過去であれば、転送鍵更新処理を中止する。次に、決済端末110は、受信した転送鍵ID 106Aと転送鍵ID 101Bとを比較し、転送鍵を更新する必要があるかどうかを判定する。もし、転送鍵ID 106Aが転送鍵ID 106Bより新しい場合は、ICカード100Bの転送鍵ID 106Bと転送鍵107Bを、ICカード100Aの転送鍵ID 106Aと転送鍵107Aに更新する処理を以下行っていく。あるいはもし、転送鍵ID 106Bが転送鍵ID 106Aより新しい場合は、ICカード100Aの転送鍵ID 106Aと転送鍵107Aを、ICカード100Bの転送鍵ID 106Bと転送鍵107Bに更新する処理を以下行っていく。あるいはもし、転送鍵ID 106Aと転送鍵ID 106Bが同一の場合は、以降の転送鍵更新処理を行わずに、直ちにバリュー転送処理に移行する。図１０は転送鍵ID 106Bが転送鍵ID 10

6Aより新しかった場合の処理フローとなっており、以下この場合について説明を行っていく。

【００４８】

また、処理S4003では、転送鍵の更新が必要であると判断したら、続いて更新鍵ID 104Aと更新鍵ID 104Bが等しいか否かを確認する。もし、等しいならば、転送鍵の更新処理に、更新鍵105Aと更新鍵105Bを用いる。もし、等しくないならば、転送鍵の更新処理に、カード秘密鍵103Aとカード秘密鍵103Bを用いる。図１０は、転送鍵の更新処理として、更新鍵を用いる場合の処理フローとなっており、以下この場合について説明を行っていく。

【００４９】

次に、決済端末110は、処理S4004として、ICカード100Aに、転送鍵更新許可要求をAPDUコマンドで送信する。ICカード100Aは、転送鍵更新許可要求を受信すると、処理S4102Aとして、更新乱数4121を生成し、これをAPDUレスポンスで、決済端末110に送信する。ここで、更新乱数4121は、不正なカードによってICカード100Aの転送鍵107Aが不正に書き換えられないように、動的認証を行うために用いる。また、更新乱数4121の乱数生成アルゴリズムは、本発明では特に規定しない。

【００５０】

次に、決済端末110は、処理S4005として、ICカード100Bに、転送鍵取得要求を、APDUコマンドで送信する。このAPDUコマンドには、更新乱数4121が含まれている。ICカード100Bは、転送鍵取得要求として、更新乱数4121を受信すると、処理S4102Bとして、更新乱数4121と、転送鍵ID 106Bと、転送鍵107Bを、更新鍵105Bで暗号化し、これをAPDUレスポンスで、決済端末110に送信する。

【００５１】

次に、決済端末は、処理S4006として、ICカード100Aに、転送鍵更新要求をAPDUコマンドで送信する。このAPDUコマンドには、更新乱数4121と、転送鍵ID 106Bと、転送鍵107Bを、更新鍵105Bで暗号化したデータが含まれている。ICカード100Aは、転送鍵更新要求として、更新乱数4121と、転送鍵ID 106Bと、転送鍵107Bを、更新鍵105Bで暗号化したデータを受信すると、処理S4103Aとして、更新鍵10

5Aで復号化し、復号された更新乱数4121が正しい値かどうかを確認する。もし、正しくない値であったなら、動的認証が失敗したと見なし、転送鍵更新処理を中止する。もし、正しい値であったなら、動的認証が成功したと見なし、処理S4104Aを行う。この処理では、転送鍵ID106Bの値が、転送鍵ID上限値112Aと転送鍵ID106Aの値との間に含まれていることを確認する。もし確認が失敗したら転送鍵の更新は行わない。もし確認が成功したら、転送鍵ID 106Aの値と転送鍵107Aの値を、転送鍵ID 106Bの値と転送鍵107Bの値に書き換える。

【００５２】

以上説明した手順において、処理S4001と、処理S4002と、処理S4003と、処理S4004と、処理S4005と、処理S4006は、決済端末110の演算制御手段303で実行する決済プログラム305により処理される。また、処理S4101Aと、処理S4102Aと、処理S4103Aと、処理S4104Aは、ICカード100Aの演算制御手段203Aで実行する決済プログラム205Aにより処理される。また、処理S4101Bと、処理S4102Bは、ICカード100Bの演算制御手段203Bで実行する決済プログラム205Bにより処理される。

【００５３】

以上の手順は、転送鍵の更新処理に、共通鍵暗号方式の鍵データである更新鍵を用いた場合であったが、次に、公開鍵暗号方式の鍵データであるカード秘密鍵を用いる場合の処理フローを、図１１を用いて説明していく。図１１の処理フローにおいては、処理S5001は処理S4001と同じである。また、処理S5002は処理S4002と同じである。また、処理S5101Aは処理S4101Aと同じである。また、処理S5101Bは処理S4101Bと同じである。

【００５４】

処理S5003においては、処理S4003と同様に、更新鍵ID 104Aと更新鍵ID 104Bが等しいか否かを確認するが、図１１は、転送鍵の更新処理として、公開鍵暗号方式を用いる場合の処理フローとなっている。したがって、更新鍵ID 104Aと更新鍵ID 104Bが等しくなかったため、転送鍵の更新処理にカード秘密鍵103Aとカード秘密鍵103Bを使用する。以下、処理S5003以降の処理について説明していく。

【００５５】

決済端末110は、処理S5004として、ICカード100Aに、転送鍵更新許可要求をAP

DUコマンドで送信する。このAPDUコマンドには、カード公開鍵証明書102Bが含まれている。ICカード100Aは、転送鍵更新許可要求として、カード公開鍵証明書102Bを受信すると、処理S3102Aとして、更新カード公開鍵証明書102BをCA公開鍵101で検証し、検証が成功したら、更新乱数5121を生成する。そして、更新乱数5121をAPDUレスポンスで、決済端末110に送信する。ここで、更新乱数5121は、不正なカードによってICカード100Aの転送鍵107Aが不正に書き換えられないように、動的認証を行うために用いる。また、更新乱数5121の乱数生成アルゴリズムは、本発明では特に規定しない。

【００５６】

次に、決済端末110は、処理S5005として、ICカード100Bに、転送鍵取得要求を、APDUコマンドで送信する。このAPDUコマンドには、カード公開鍵証明書102Aと、更新乱数5121が含まれている。ICカード100Bは、転送鍵取得要求として、カード公開鍵証明書102Aと、更新乱数5121を受信すると、処理S5102Bとして、まず、カード公開鍵証明書102Aを、CA公開鍵101で検証する。検証が成功したら、転送鍵ID 106Bと転送鍵107Bを、カード公開鍵証明書102Aに含まれるカード公開鍵で暗号化する。次に、処理S5103Bとして、カード秘密鍵103Bを用いて、転送鍵ID 106Bと転送鍵107Bを暗号化したデータと、更新乱数5121とに対するデジタル署名5122を生成する。そして、転送鍵ID 106Bと転送鍵107Bを暗号化したデータと、デジタル署名5122を、APDUレスポンスで、決済端末110に送信する。ここで、デジタル署名5122の作成アルゴリズムは、公開鍵暗号方式に基づいたものであれば、どのようなアルゴリズムでも本発明の適用範囲である。

【００５７】

次に、決済端末は、処理S5006として、ICカード100Aに、転送鍵更新要求をAPDUコマンドで送信する。このAPDUコマンドには、デジタル署名5122と、転送鍵ID 106Bと転送鍵107Bを暗号化したデータとが含まれている。ICカード100Aは、転送鍵更新要求として、デジタル署名5122と、転送鍵ID 106Bと転送鍵107Bを暗号化したデータを受信すると、まず、処理S5103Aとして、カード公開鍵102Bを用いて、デジタル署名5122の検証を行う。この検証が成功したら、動的認証が成功したと見なし、次に、処理S5104Aとして、転送鍵ID 106Bと転送鍵107Bを、カード秘

密鍵103Aで復号化する。そして、処理S5105Aを行う。この処理では、転送鍵ID106Bの値が、転送鍵ID上限値112Aと転送鍵ID106Aの値との間に含まれていることを確認する。もし確認が失敗したら転送鍵の更新は行わない。もし確認が成功したら、転送鍵ID 106Aの値と転送鍵107Aの値を、転送鍵ID 106Bの値と転送鍵107Bの値に書き換える。

【００５８】

以上説明した手順において、処理S5001と、処理S5002と、処理S5003と、処理S5004と、処理S5005と、処理S5006は、決済端末110の演算制御手段303で実行する決済プログラム305により処理される。また、処理S5101Aと、処理S5102Aと、処理S5103Aと、処理S5104Aと、処理S5105Aは、ICカード100Aの演算制御手段203Aで実行する決済プログラム205Aにより処理される。また、処理S5101Bと、処理S5102Bと、処理S5103Bは、ICカード100Bの演算制御手段203Bで実行する決済プログラム205Bにより処理される。

【００５９】

以上の手順により、転送鍵をより新しい値に、安全に書き換えることができる。本発明に係わる第3の実施例においては、ICカード100AとICカード100Bとの間で、転送鍵が異なっていても、同一の更新鍵を共有していれば、これらの更新鍵を用いて、両カード内の転送鍵の値を、新しい値に更新することが可能になる。また、同一の更新鍵を共有していない場合でも、カード公開鍵およびカード秘密鍵を用いて、両カード内の転送鍵の値を、新しい値に更新することが可能になる。例えば、有効期限が切れたICカードを、新しいICカードに切替える時に、転送鍵を新しい値に更新しておけば、この新しいICカードとバリュー転送を行った、古いICカードの転送鍵の値を、更新鍵を使って新しい値に更新することができる。この時の転送鍵の更新は、共通鍵暗号方式を使って行うため、短時間に処理を完了することが可能である。さらに、新しいICカードに切替える時に、更新鍵も新しい値に更新することも可能である。この場合は、新しいカードと古いカードの間で更新鍵が異なってしまうが、カード公開鍵およびカード秘密鍵を用いて、転送鍵を更新することが可能になる。

【００６０】

また、本実施例においては、CA公開鍵および公開鍵証明書を用いるため、第2の実施例で説明したように、CRLを用いて、無効となった公開鍵証明書を保持しているICカードとはバリュー転送を行わないようにすることも可能である。例えば、決済端末110がCRLを保持していて、ICカード100Aから取得したカード公開鍵証明書102Aと、ICカード100Bから取得したカード公開鍵証明書102Bのチェックを、CRLを用いて行う場合も、本発明の適用範囲である。

【００６１】

次に、本発明に係わる第４の実施例について説明する。本実施例においては、それぞれのICカードが転送鍵を複数保持している。図１２は、本実施例におけるバリュー転送システムの構成要素ブロック図であるが、これは、第1の実施例で説明した図1のブロック図と同じ構成となっている。次に、ICカード100Aの鍵情報204Aの詳細について説明する。

【００６２】

図１３は鍵情報204Aのデータ構成図である。図１３において、鍵情報204Aは、更新鍵105Aと、転送鍵ID 106Aと、転送鍵107Aと、転送鍵ID[1] 106A1と、転送鍵ID[2] 106A2と、転送鍵[1] 107A1と、転送鍵[2] 107A2バリュー残高108Aと、有効期限111Aを含んでいる。また、ICカード100Bも同様のデータ構成となる。ここで、更新鍵105Aは転送鍵107Aを更新するために用いる共通鍵暗号方式の鍵データであり、転送鍵107Aの暗号化および復号化を行う時に用いる。また、転送鍵ID 106Aは転送鍵107Aを一意に識別するための番号であり、転送鍵の新旧を値の大小で判別する。例えば、転送鍵IDの値が大きいほど新しい転送鍵と見なす。また、転送鍵ID[1] 106A1は、転送鍵[1] 107A1を一意に識別するための番号である。また、転送鍵ID[2] 106A1は、転送鍵[2] 107A1を一意に識別するための番号である。また、転送鍵[1]107A1および転送鍵[2]107A2は、バリューを転送するために用いる共通鍵暗号方式の鍵データである。本実施例においては、転送鍵ID106Aの値は、転送鍵ID[1] 106A1あるいは転送鍵ID[2] 106A2のいずれかの値をとり、現在使用している転送鍵のIDを表す。例えば、転送鍵ID106Aの値が、転送鍵ID[1] 106A1の値と等しい場合は、バリュー転送には転送鍵[1] 107A1を用いる。なお、更新鍵105Bと、転送鍵[1] 107A1と、転送鍵[2]107A2は、外部からの読出しが行え

ないものとする。また、図１３においては、ICカードが保持している転送鍵の数は２個となっているが、転送鍵を２個以上保持している場合も、本発明の適用範囲である。

【００６３】

次に、本実施例に係わる、転送鍵を更新するための処理を詳細に説明していく。この処理は、バリュー転送を行う前に実行する。また、決済端末110がICカード100AおよびICカード100Bに送信するコマンドはAPDU形式を用いるものとして説明していく。図１４は、転送鍵を更新するための処理フロー図である。まず、決済端末110は、処理S6001として、ICカード100AおよびICカード100Bに格納されている、決済サービスプログラムを選択起動するために、決済サービス選択要求をAPDUコマンドで送信する。

【００６４】

次に、決済端末110は、処理S6002として、ICカード100AおよびICカード100Bにカード情報取得要求をAPDUコマンドで送信する。ICカード100Aは、カード情報取得要求を受信すると、処理S6101Aとして、転送鍵ID 106Aと有効期限111Aを、決済端末110にAPDUレスポンスで送信する。同様に、ICカード100Bは、カード情報取得要求を受信すると、処理S6101Bとして、転送鍵ID 106Bと有効期限111Bを決済端末110にAPDUレスポンスで送信する。

【００６５】

次に、決済端末110は、処理S6003として転送鍵更新チェックを行う。この処理では、まず、受信した有効期限111Aと有効期限111Bとを調べ、いずれも現在の日付より未来であることを確認する。もし、いずれかが、現在の日付より過去であれば、転送鍵更新処理を中止する。次に、決済端末110は、受信した転送鍵ID 106Aと転送鍵ID 106Bとを比較し、転送鍵を更新する必要があるかどうかを判定する。もし、転送鍵ID 106Aが転送鍵ID 106Bより新しい場合は、ICカード100Bの転送鍵ID 106Bと転送鍵107Bを、ICカード100Aの転送鍵ID 106Aと転送鍵107Aに更新する処理を以下行っていく。あるいはもし、転送鍵ID 106Bが転送鍵ID 106Aより新しい場合は、ICカード100Aの転送鍵ID 106Aと転送鍵107Aを、ICカード100Bの転送鍵ID 106Bと転送鍵107Bに更新する処理を以下行っていく。あるいはもし、

転送鍵ID 106Aと転送鍵ID 106Bが同一の場合は、以降の転送鍵更新処理を行わずに、直ちにバリュー転送処理に移行する。図１４は転送鍵ID 106Bが転送鍵ID 106Aより新しかった場合の処理フローとなっており、以下この場合について説明を行っていく。

【００６６】

次に、決済端末110は、処理S6004として、ICカード100Aに、転送鍵更新許可要求をAPDUコマンドで送信する。ICカード100Aは、転送鍵更新許可要求を受信すると、処理S6102Aとして、更新乱数6121を生成し、これをAPDUレスポンスで、決済端末110に送信する。ここで、更新乱数6121は、不正なカードによってICカード100Aの転送鍵ID106Aが不正に書き換えられないように、動的認証を行うために用いる。また、更新乱数1121の乱数生成アルゴリズムは、本発明では特に規定しない。

【００６７】

次に、決済端末110は、処理S6005として、ICカード100Bに、転送鍵取得要求を、APDUコマンドで送信する。このAPDUコマンドには、更新乱数6121が含まれている。ICカード100Bは、転送鍵取得要求として、更新乱数6121を受信すると、処理S6102Bとして、更新乱数6121と、転送鍵ID 106Bを、更新鍵105Bで暗号化し、これをAPDUレスポンスで、決済端末110に送信する。

【００６８】

次に、決済端末は、処理S6006として、ICカード100Aに、転送鍵更新要求をAPDUコマンドで送信する。このAPDUコマンドには、更新乱数6121と、転送鍵ID 106Bを、更新鍵105Bで暗号化したデータが含まれている。ICカード100Aは、転送鍵更新要求として、更新乱数6121と転送鍵ID 106Bを、更新鍵105Bで暗号化したデータを受信すると、処理S6103Aとして、更新鍵105Aで復号化し、復号された更新乱数6121が正しい値かどうかを確認する。もし、正しくない値であったなら、動的認証が失敗したと見なし、転送鍵更新処理を中止する。もし、正しい値であったなら、動的認証が成功したと見なし、処理S6104Aを行う。この処理では、受信した転送鍵ID 106Bの値が、転送鍵ID106Aの値より新しく、且つ、転送鍵ID[1]106A1か転送鍵ID[2]106A2のいずれかの値に等しいことを確認する。もし確認が失敗

したら転送鍵の更新は行わない。もし確認が成功したら、転送鍵ID 106Aの値を、転送鍵ID 106Bの値に書き換える。

【００６９】

以上説明した手順において、処理S6001と、処理S6002と、処理S6003と、処理S6004と、処理S6005と、処理S6006は、決済端末110の演算制御手段303で実行する決済プログラム305により処理される。また、処理S6101Aと、処理S6102Aと、処理S6103Aと、処理S6104Aは、ICカード100Aの演算制御手段203Aで実行する決済プログラム205Aにより処理される。また、処理S6101Bと、処理S6102Bは、ICカード100Bの演算制御手段203Bで実行する決済プログラム205Bにより処理される。

【００７０】

以上の手順により、転送鍵をより新しい値に、安全に更新することができる。また、転送鍵の更新は、共通鍵暗号方式を使って行うため、短時間に処理を完了することが可能である。

【００７１】

以上、説明を行ってきた本発明に係わる第４の実施例においては、ICカード100AとICカード100Bに予め複数の転送鍵を格納しておくため、更新する転送鍵の値は、ICカード間で送受信する必要がない。したがって、他の実施例に比べてよりセキュリティを向上することが可能になる。ここで、本実施例では、転送鍵の更新に、第１の実施例と同様に更新鍵を用いたが、第２の実施例と同様にカード公開鍵およびカード秘密鍵を用いたとしても、本発明の適用範囲である。また、第３の実施例と同様に更新鍵と、カード公開鍵およびカード秘密鍵を併用したとしても、本発明の適用範囲である。

【００７２】

次に、本発明に係わる第５の実施例について説明する。本実施例においては、転送鍵の更新に、共通鍵暗号方式と公開鍵暗号方式のどちらを用いるかを選択できるようになっている。また、転送鍵を更新するために用いる更新鍵の値が、ICカード間で異なっている場合は、更新鍵の更新処理も行う。図１５は、本実施例におけるバリュー転送システムの構成要素ブロック図であるが、これは、第1の実施例で説明した図1のブロック図と同じ構成となっている。次に、ICカード100

Aの鍵情報204Aの詳細について説明する。

【００７３】

図１６は鍵情報204Aのデータ構成図である。図１６において、鍵情報204Aは、CA公開鍵101と、カード公開鍵証明書102Aと、カード秘密鍵103Aと、更新鍵ID 104Aと、更新鍵105Aと、転送鍵ID 106Aと、転送鍵107Aと、転送鍵ID上限値112Aと、更新鍵ID上限値113Aを含んでいる。また、ICカード100Bも同様のデータ構成となる。ここで、CA公開鍵101は、任意の認証局の公開鍵であり、カード公開鍵証明書102Aを検証するために用いる。カード公開鍵証明書102Aは、カード秘密鍵103Aと対の鍵データであるカード公開鍵の正当性を証明するためのデータであり、このカード公開鍵はカード公開鍵証明書102Aの内部に含まれている構成となっている。カード秘密鍵103Aは、公開鍵暗号方式の秘密鍵であり、転送鍵を更新するために用いる。また、更新鍵ID104Aは、更新鍵105Aを一意に識別するための番号であり、更新鍵の新旧を値の大小で判別する。例えば、更新鍵IDの値が大きいほど新しい更新鍵と見なす。更新鍵105Aは転送鍵107Aを更新するために用いる共通鍵暗号方式の鍵データであり、転送鍵107Aの暗号化および復号化を行う時に用いる。また、転送鍵ID 106Aは転送鍵107Aを一意に識別するための番号であり、転送鍵の新旧を値の大小で判別する。例えば、転送鍵IDの値が大きいほど新しい転送鍵と見なす。また、転送鍵107Aは、バリューを転送するために用いる共通鍵暗号方式の鍵データである。転送鍵ID上限値 112Aは、ICカード100Aに格納可能な転送鍵ID106Aの値の上限値を表すデータでる。更新鍵ID上限値 113Aは、ICカード100Aに格納可能な更新鍵ID106Aの値の上限値を表すデータでる。なお、更新鍵105A、および転送鍵107Aを用いる暗号アルゴリズムは、共通鍵暗号方式であれば、どのようなアルゴリズムを用いても本発明の適用範囲である。また、CA公開鍵101、カード公開鍵証明書102A、カード秘密鍵103Aを用いる暗号アルゴリズムは、公開鍵暗号方式であれば、どのようなアルゴリズムを用いても本発明の適用範囲である。また、カード秘密鍵103Aと、更新鍵104Aと、転送鍵107Aは、ICカード100A外部からの読出しが行えないものとする。

【００７４】

次に、本実施例に係わる、転送鍵を更新するための処理を詳細に説明していく

。この処理は、バリュー転送を行う前に実行する。また、決済端末110がICカード100AおよびICカード100Bに送信するコマンドはAPDU形式を用いるものとして説明していく。図１７は、転送鍵を更新するための処理フロー図である。まず、決済端末110は、処理S7001として、ICカード100AおよびICカード100Bに格納されている、決済サービスプログラムを選択起動するために、決済サービス選択要求をAPDUコマンドで送信する。

【００７５】

次に、決済端末110は、処理S7002として、ICカード100AおよびICカード100Bにカード情報取得要求をAPDUコマンドで送信する。ICカード100Aは、カード情報取得要求を受信すると、処理S7101Aとして、カード公開鍵証明書102Aと更新鍵ID 104Aと転送鍵ID 106Aと有効期限111Aを、決済端末110にAPDUレスポンスで送信する。同様に、ICカード100Bは、カード情報取得要求を受信すると、処理S4101Bとして、カード公開鍵証明書102Bと更新鍵ID 104Bと転送鍵ID 106Bと有効期限111Bを決済端末110にAPDUレスポンスで送信する。

【００７６】

次に、決済端末110は、処理S7003として転送鍵更新チェックを行う。この処理では、まず、受信した有効期限111Aと有効期限111Bとを調べ、いずれも現在の日付より未来であることを確認する。もし、いずれかが、現在の日付より過去であれば、転送鍵更新処理を中止する。次に、決済端末110は、受信した転送鍵ID 106Aと転送鍵ID 101Bとを比較し、転送鍵を更新する必要があるかどうかを判定する。もし、転送鍵ID 106Aが転送鍵ID 106Bより新しい場合は、ICカード100Bの転送鍵ID 106Bと転送鍵107Bを、ICカード100Aの転送鍵ID 106Aと転送鍵107Aに更新する処理を以下行っていく。あるいはもし、転送鍵ID 106Bが転送鍵ID 106Aより新しい場合は、ICカード100Aの転送鍵ID 106Aと転送鍵107Aを、ICカード100Bの転送鍵ID 106Bと転送鍵107Bに更新する処理を以下行っていく。あるいはもし、転送鍵ID 106Aと転送鍵ID 106Bが同一の場合は、以降の転送鍵更新処理を行わずに、直ちにバリュー転送処理に移行する。図１７は転送鍵ID 106Bが転送鍵ID 106Aより新しかった場合の処理フローとなっており、以下この場合について説明を行っていく。

【００７７】

また、処理S7003では、転送鍵の更新が必要であると判断したら、続いて更新鍵ID 104Aと更新鍵ID 104Bが等しいか否かを確認する。もし、等しいならば、転送鍵の更新処理に、更新鍵105Aと更新鍵105Bを用いる。もし、等しくないならば、転送鍵と更新鍵の更新処理に、カード秘密鍵103Aとカード秘密鍵103Bを用いる。図１７は、転送鍵の更新処理として、更新鍵を用いる場合の処理フローとなっており、以下この場合について説明を行っていく。

【００７８】

次に、決済端末110は、処理S7004として、ICカード100Aに、転送鍵更新許可要求をAPDUコマンドで送信する。ICカード100Aは、転送鍵更新許可要求を受信すると、処理S7102Aとして、更新乱数7121を生成し、これをAPDUレスポンスで、決済端末110に送信する。ここで、更新乱数7121は、不正なカードによってICカード100Aの転送鍵107Aが不正に書き換えられないように、動的認証を行うために用いる。また、更新乱数7121の乱数生成アルゴリズムは、本発明では特に規定しない。

【００７９】

次に、決済端末110は、処理S7005として、ICカード100Bに、転送鍵取得要求を、APDUコマンドで送信する。このAPDUコマンドには、更新乱数7121が含まれている。ICカード100Bは、転送鍵取得要求として、更新乱数7121を受信すると、処理S7102Bとして、更新乱数7121と、転送鍵ID 106Bと、転送鍵107Bを、更新鍵105Bで暗号化し、これをAPDUレスポンスで、決済端末110に送信する。

【００８０】

次に、決済端末は、処理S7006として、ICカード100Aに、転送鍵更新要求をAPDUコマンドで送信する。このAPDUコマンドには、更新乱数7121と、転送鍵ID 106Bと、転送鍵107Bを、更新鍵105Bで暗号化したデータが含まれている。ICカード100Aは、転送鍵更新要求として、更新乱数7121と、転送鍵ID 106Bと、転送鍵107Bを、更新鍵105Bで暗号化したデータを受信すると、処理S7103Aとして、更新鍵105Aで復号化し、復号された更新乱数7121が正しい値かどうかを確認する。もし、正しくない値であったなら、動的認証が失敗したと見なし、転送鍵更新処理を中

止する。もし、正しい値であったなら、動的認証が成功したと見なし、処理S7104Aを行う。この処理では、転送鍵ID106Bの値が、転送鍵ID上限値112Aと転送鍵ID106Aの値との間に含まれていることを確認する。もし確認が失敗したら転送鍵の更新は行わない。もし確認が成功したら、転送鍵ID 106Aの値と転送鍵107Aの値を、転送鍵ID 106Bの値と転送鍵107Bの値に書き換える。

【００８１】

以上説明した手順において、処理S7001と、処理S7002と、処理S7003と、処理S7004と、処理S7005と、処理S7006は、決済端末110の演算制御手段303で実行する決済プログラム305により処理される。また、処理S7101Aと、処理S7102Aと、処理S7103Aと、処理S7104Aは、ICカード100Aの演算制御手段203Aで実行する決済プログラム205Aにより処理される。また、処理S7101Bと、処理S7102Bは、ICカード100Bの演算制御手段203Bで実行する決済プログラム205Bにより処理される。

【００８２】

以上の手順は、転送鍵の更新処理に、共通鍵暗号方式の鍵データである更新鍵を用いた場合であったが、次に、公開鍵暗号方式の鍵データであるカード秘密鍵を用いる場合の処理フローを、図１８を用いて説明していく。図１８の処理フローにおいては、処理S8001は処理S7001と同じである。また、処理S8002は処理S7002と同じである。また、処理S8101Aは処理S7101Aと同じである。また、処理S8101Bは処理S7101Bと同じである。

【００８３】

処理S8003においては、処理S7003と同様に、更新鍵ID 104Aと更新鍵ID 104Bが等しいか否かを確認するが、図１８は、更新鍵ID 104Aと更新鍵ID 104Bが異なっているために、転送鍵と更新鍵の更新処理として、公開鍵暗号方式を用いる場合の処理フローとなっている。したがって、転送鍵と更新鍵の更新処理にカード秘密鍵103Aとカード秘密鍵103Bを使用する。以下、処理S8003以降の処理について説明していく。

【００８４】

決済端末110は、処理S8004として、ICカード100Aに、転送鍵更新許可要求をAPDUコマンドで送信する。このAPDUコマンドには、カード公開鍵証明書102Bが含ま

れている。ICカード100Aは、転送鍵更新許可要求として、カード公開鍵証明書102Bを受信すると、処理S8102Aとして、更新カード公開鍵証明書102BをCA公開鍵101で検証し、検証が成功したら、更新乱数8121を生成する。そして、更新乱数8121をAPDUレスポンスで、決済端末110に送信する。ここで、更新乱数8121は、不正なカードによってICカード100Aの転送鍵107Aが不正に書き換えられないように、動的認証を行うために用いる。また、更新乱数8121の乱数生成アルゴリズムは、本発明では特に規定しない。

【００８５】

次に、決済端末110は、処理S8005として、ICカード100Bに、転送鍵取得要求を、APDUコマンドで送信する。このAPDUコマンドには、カード公開鍵証明書102Aと、更新乱数8121が含まれている。ICカード100Bは、転送鍵取得要求として、カード公開鍵証明書102Aと、更新乱数8121を受信すると、処理S8102Bとして、まず、カード公開鍵証明書102Aを、CA公開鍵101で検証する。検証が成功したら、更新鍵ID 104Bと更新鍵105Bと転送鍵ID 106Bと転送鍵107Bを、カード公開鍵証明書102Aに含まれるカード公開鍵で暗号化する。次に、処理S8103Bとして、カード秘密鍵103Bを用いて、更新鍵ID 104Bと更新鍵105Bと転送鍵ID 106Bと転送鍵107Bを暗号化したデータと、更新乱数8121とに対するデジタル署名8122を生成する。そして、更新鍵ID 104Bと更新鍵105Bと転送鍵ID 106Bと転送鍵107Bを暗号化したデータと、デジタル署名8122を、APDUレスポンスで、決済端末110に送信する。ここで、デジタル署名8122の作成アルゴリズムは、公開鍵暗号方式に基づいたものであれば、どのようなアルゴリズムでも本発明の適用範囲である。

【００８６】

次に、決済端末は、処理S8006として、ICカード100Aに、転送鍵更新要求をAPDUコマンドで送信する。このAPDUコマンドには、デジタル署名8122と、更新鍵ID 104Bと更新鍵105Bと転送鍵ID 106Bと転送鍵107Bを暗号化したデータとが含まれている。ICカード100Aは、転送鍵更新要求として、デジタル署名8122と、更新鍵ID 104Bと更新鍵105Bと転送鍵ID 106Bと転送鍵107Bを暗号化したデータを受信すると、まず、処理S8103Aとして、カード公開鍵102Bを用いて、デジタル署名8122の検証を行う。この検証が成功したら、動的認証が成功したと見なし、次に、処

理S8104Aとして、転更新鍵ID 104Bと更新鍵105Bと送鍵ID 106Bと転送鍵107Bを、カード秘密鍵103Aで復号化する。そして、処理S8105Aを行う。この処理では、更新鍵ID104Bの値が、更新鍵ID上限値113Aと更新鍵ID104Aの値との間に含まれ、且つ、転送鍵ID106Bの値が、転送鍵ID上限値112Aと転送鍵ID106Aの値との間に含まれていることを確認する。もし確認が失敗したら転送鍵の更新は行わない。もし確認が成功したら、更新鍵ID 104Aの値と更新鍵105Aの値を、更新鍵ID 104Bの値と更新鍵105Bの値に書き換える。また、転送鍵ID 106Aの値と転送鍵107Aの値を、転送鍵ID 106Bの値と転送鍵107Bの値に書き換える。

【００８７】

以上説明した手順において、処理S8001と、処理S8002と、処理S8003と、処理S8004と、処理S8005と、処理S8006は、決済端末110の演算制御手段303で実行する決済プログラム305により処理される。また、処理S8101Aと、処理S8102Aと、処理S8103Aと、処理S8104Aと、処理S8105Aは、ICカード100Aの演算制御手段203Aで実行する決済プログラム205Aにより処理される。また、処理S8101Bと、処理S8102Bと、処理S8103Bは、ICカード100Bの演算制御手段203Bで実行する決済プログラム205Bにより処理される。

【００８８】

以上の手順により、転送鍵をより新しい値に、安全に書き換えることができる。本発明に係わる第5の実施例においては、ICカード100AとICカード100Bとの間で、転送鍵が異なっていても、同一の更新鍵を共有していれば、これらの更新鍵を用いて、両カード内の転送鍵の値を、新しい値に更新することが可能になる。また、同一の更新鍵を共有していない場合でも、カード公開鍵およびカード秘密鍵を用いて、両カード内の更新鍵と転送鍵の値を、新しい値に更新することが可能になる。例えば、有効期限が切れたICカードを、新しいICカードに切替える時に、転送鍵を新しい値に更新しておけば、この新しいICカードとバリュー転送を行った、古いICカードの転送鍵の値を、更新鍵を使って新しい値に更新することができる。この時の転送鍵の更新は、共通鍵暗号方式を使って行うため、短時間に処理を完了することが可能である。さらに、新しいICカードに切替える時に、更新鍵も新しい値に更新することも可能である。この場合は、新しいカードと古

いカードの間で更新鍵が異なってしまうが、カード公開鍵およびカード秘密鍵を用いて、更新鍵と転送鍵を更新することが可能になる。

【００８９】

なお、以上の各実施例での説明において転送鍵ID上限値を設定したが、必須ではない。設定しない場合、何度でも更新できるので長期間に渡りICカードを利用することができる。一方、上述のように設定した場合、ICカードに一定の有効期間を持たせることができ、上限値に達した時点でICカードを回収することができる。

【００９０】

また、以上の各実施例で説明したとおり、本発明によればシステム全体のセキュリティを向上できるが、例えば、あるシステムで転送鍵が漏洩してしまった場合、従来の転送鍵の更新が不可能なシステムではセキュリティを失ってしまう。回復するには全てのICカードを回収し新たな転送鍵を設定する必要がある。一方本発明によれば、バリュー転送の前処理として転送鍵を更新することができるので、全てのICカードを回収するということなく、新たな転送鍵の設定をすることができる。従って万一転送鍵が漏洩した場合でも容易にセキュリティを回復することができる。また、転送鍵が漏洩した場合でなくとも定期的に転送鍵を更新するようにすればセキュリティをさらに向上することができる。

【００９１】

【発明の効果】

以上説明したように、本発明によれば、ICカード間のバリュー転送に、共通鍵暗号方式を用いた場合に、バリュー転送で使用する暗号鍵を容易に更新可能にすることで、システム全体のセキュリティを向上できるICカードおよび決済端末を提供することができる。

【図面の簡単な説明】

【図１】第１の実施例に係わる、バリュー転送システムの構成要素ブロック図である。

【図２】第1の実施例に係わる、鍵情報のデータ構成図である。

【図３】第１の実施例に係わる、転送鍵更新の処理フローである。

【図４】バリュー転送の処理フローである。

【図５】第2の実施例に係わる、バリュー転送システムの構成要素ブロック図である。

【図６】第2の実施例に係わる、鍵情報のデータ構成図である。

【図７】第2の実施例に係わる、転送鍵更新の処理フローである。

【図８】第3の実施例に係わる、バリュー転送システムの構成要素ブロック図である。

【図９】第3の実施例に係わる、鍵情報のデータ構成図である。

【図１０】第3の実施例に係わる、共通鍵暗号方式を用いた転送鍵更新の処理フローである。

【図１１】第3の実施例に係わる、公開鍵暗号方式を用いた転送鍵更新の処理フローである。

【図１２】第4の実施例に係わる、バリュー転送システムの構成要素ブロック図である。

【図１３】第4の実施例に係わる、鍵情報のデータ構成図である。

【図１４】第4の実施例に係わる、転送鍵更新の処理フローである。

【図１５】第5の実施例に係わる、バリュー転送システムの構成要素ブロック図である。

【図１６】第5の実施例に係わる、鍵情報のデータ構成図である。

【図１７】第5の実施例に係わる、共通鍵暗号方式を用いた転送鍵更新の処理フローである。

【図１８】第5の実施例に係わる、公開鍵暗号方式を用いた転送鍵更新の処理フローである。

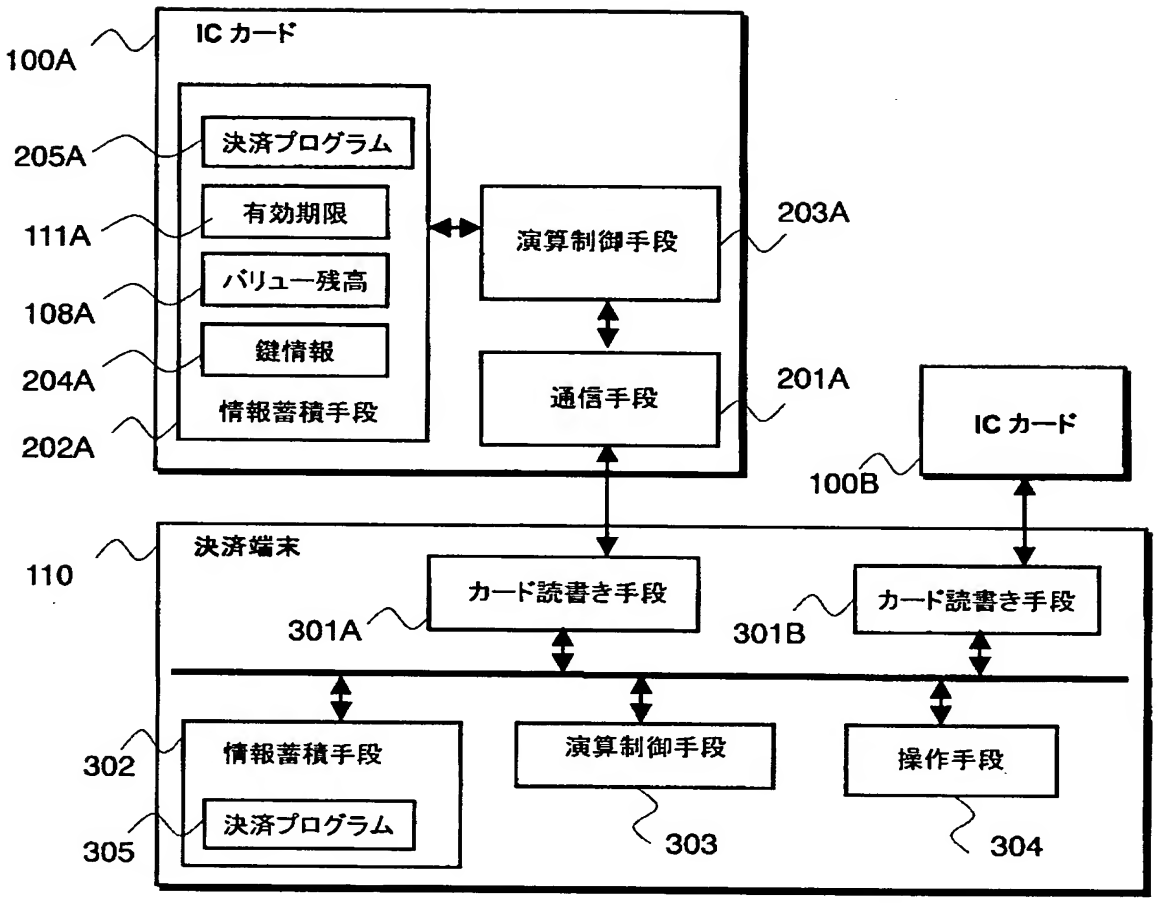
【符号の説明】

100A…ICカード、100B…ICカード、110…決済端末、201A…通信手段、202A…情報蓄積手段、203A…演算制御手段、111A…有効期限、108B…バリュー残高、204A…鍵情報、301A…カード読書き手段、301B…カード読書き手段、302…情報蓄積手段、303…演算制御手段、304…操作手段

【書類名】図面

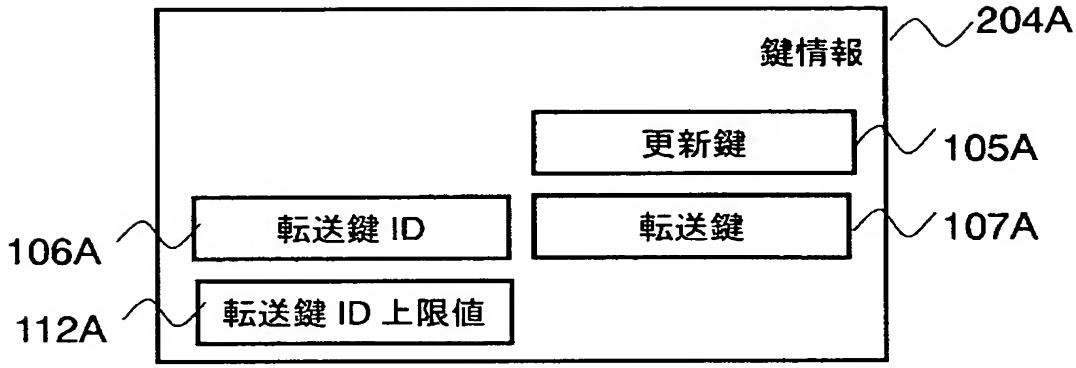
【図１】

図　1


ICカード
100A
決済プログラム
205A
有効期限
111A
バリュー残高
108A
鍵情報
204A
情報蓄積手段
202A
演算制御手段
203A
通信手段
201A
ICカード
100B
決済端末
110
カード読書き手段
301A
カード読書き手段
301B
情報蓄積手段
302
決済プログラム
305
演算制御手段
303
操作手段
304

【図２】

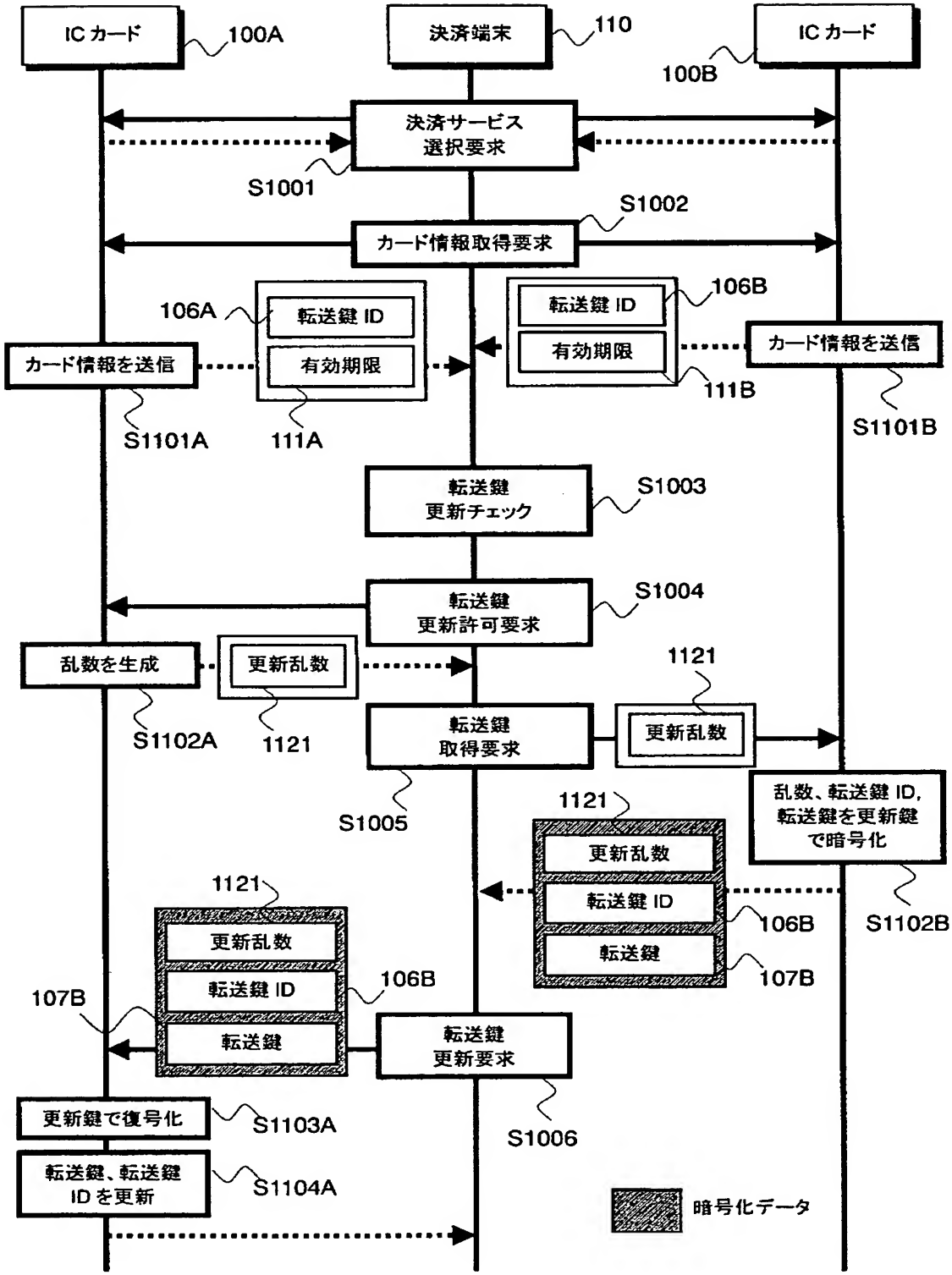
図 2



出証特２００３－３０１６５３５

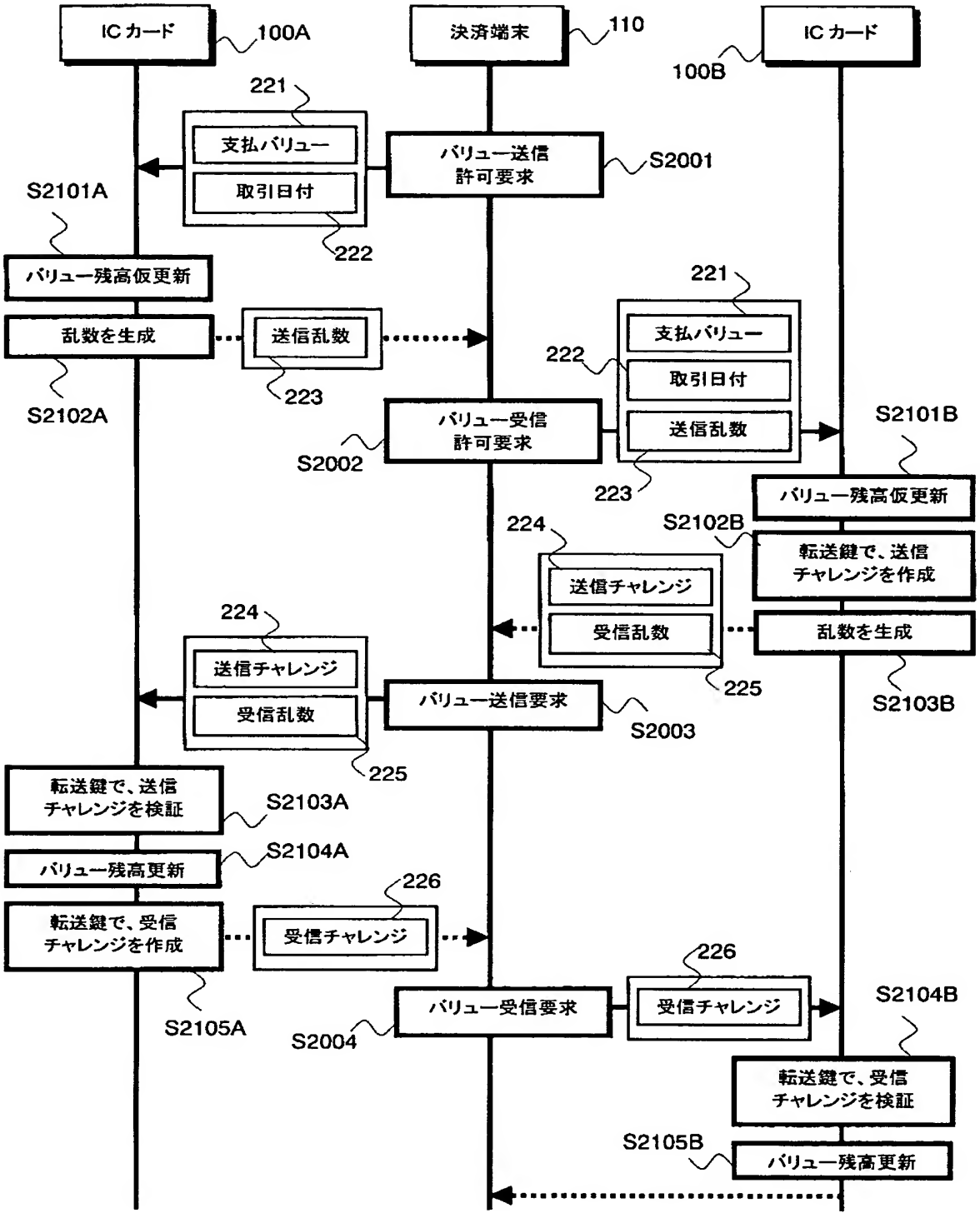
【図３】

図 3


ICカード
100A
決済端末
110
ICカード
100B
決済サービス
選択要求
S1001
S1002
カード情報取得要求
106A
転送鍵 ID
有効期限
カード情報を送信
S1101A
111A
転送鍵 ID
有効期限
106B
111B
カード情報を送信
S1101B
転送鍵
更新チェック
S1003
転送鍵
更新許可要求
S1004
乱数を生成
更新乱数
S1102A
1121
1121
転送鍵
取得要求
更新乱数
S1005
乱数、転送鍵 ID,
転送鍵を更新鍵
で暗号化
S1102B
1121
更新乱数
転送鍵 ID
転送鍵
106B
107B
1121
更新乱数
転送鍵 ID
転送鍵
106B
107B
転送鍵
更新要求
S1006
更新鍵で復号化
S1103A
転送鍵、転送鍵
IDを更新
S1104A
暗号化データ

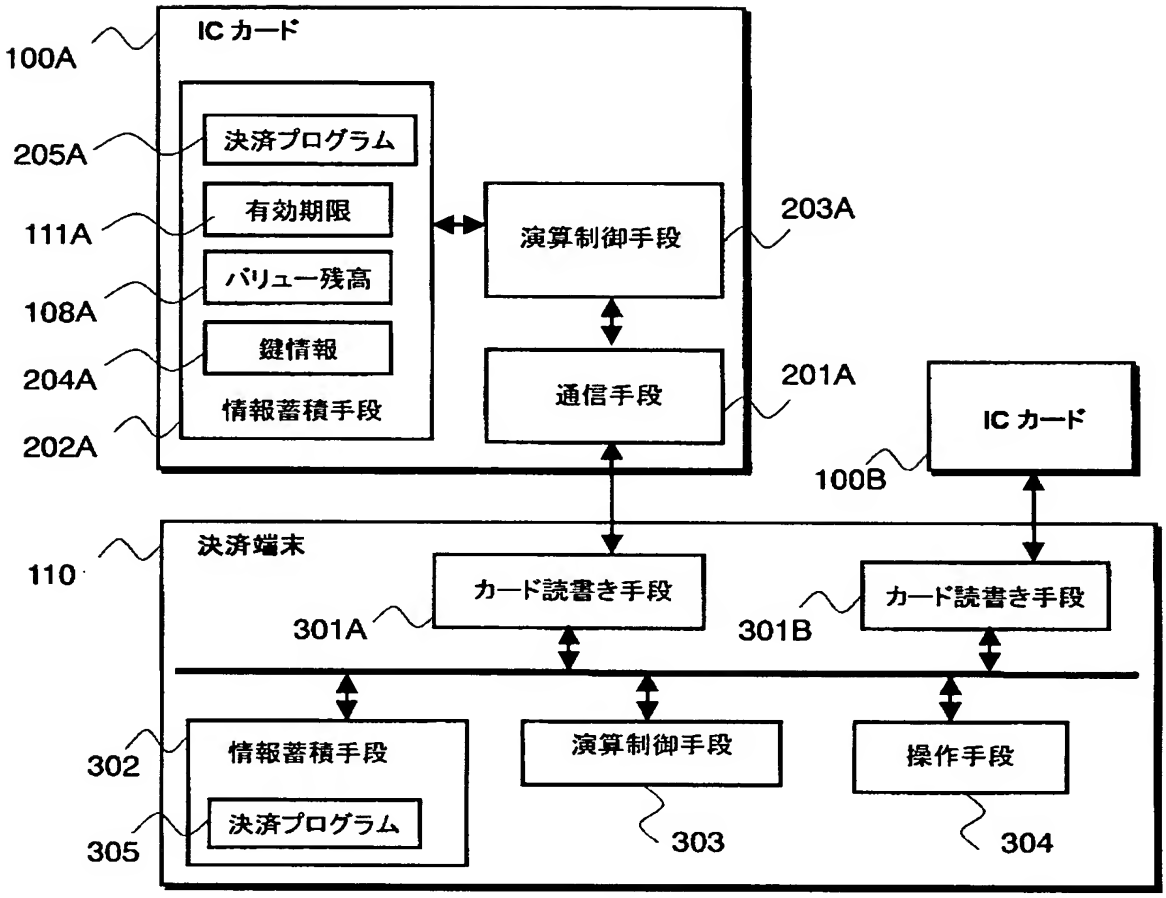
【図４】

図　4


ICカード
100A
決済端末
110
ICカード
100B
221
支払バリュー
取引日付
222
バリュー送信
許可要求
S2001
S2101A
バリュー残高仮更新
乱数を生成
S2102A
送信乱数
223
221
支払バリュー
222
取引日付
送信乱数
223
バリュー受信
許可要求
S2002
S2101B
バリュー残高仮更新
S2102B
転送鍵で、送信
チャレンジを作成
224
送信チャレンジ
受信乱数
225
乱数を生成
S2103B
224
送信チャレンジ
受信乱数
225
バリュー送信要求
S2003
転送鍵で、送信
チャレンジを検証
S2103A
バリュー残高更新
S2104A
226
転送鍵で、受信
チャレンジを作成
受信チャレンジ
S2105A
226
バリュー受信要求
S2004
受信チャレンジ
S2104B
転送鍵で、受信
チャレンジを検証
S2105B
バリュー残高更新

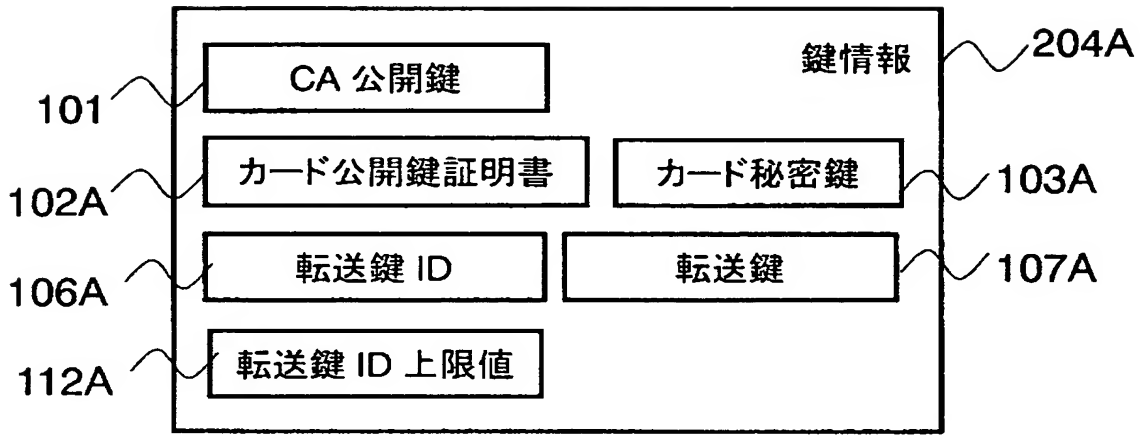
【図５】

図 5


ICカード
100A
決済プログラム
205A
有効期限
111A
バリュー残高
108A
鍵情報
204A
情報蓄積手段
202A
演算制御手段
203A
通信手段
201A
ICカード
100B
決済端末
110
カード読書き手段
301A
カード読書き手段
301B
情報蓄積手段
302
決済プログラム
305
演算制御手段
303
操作手段
304

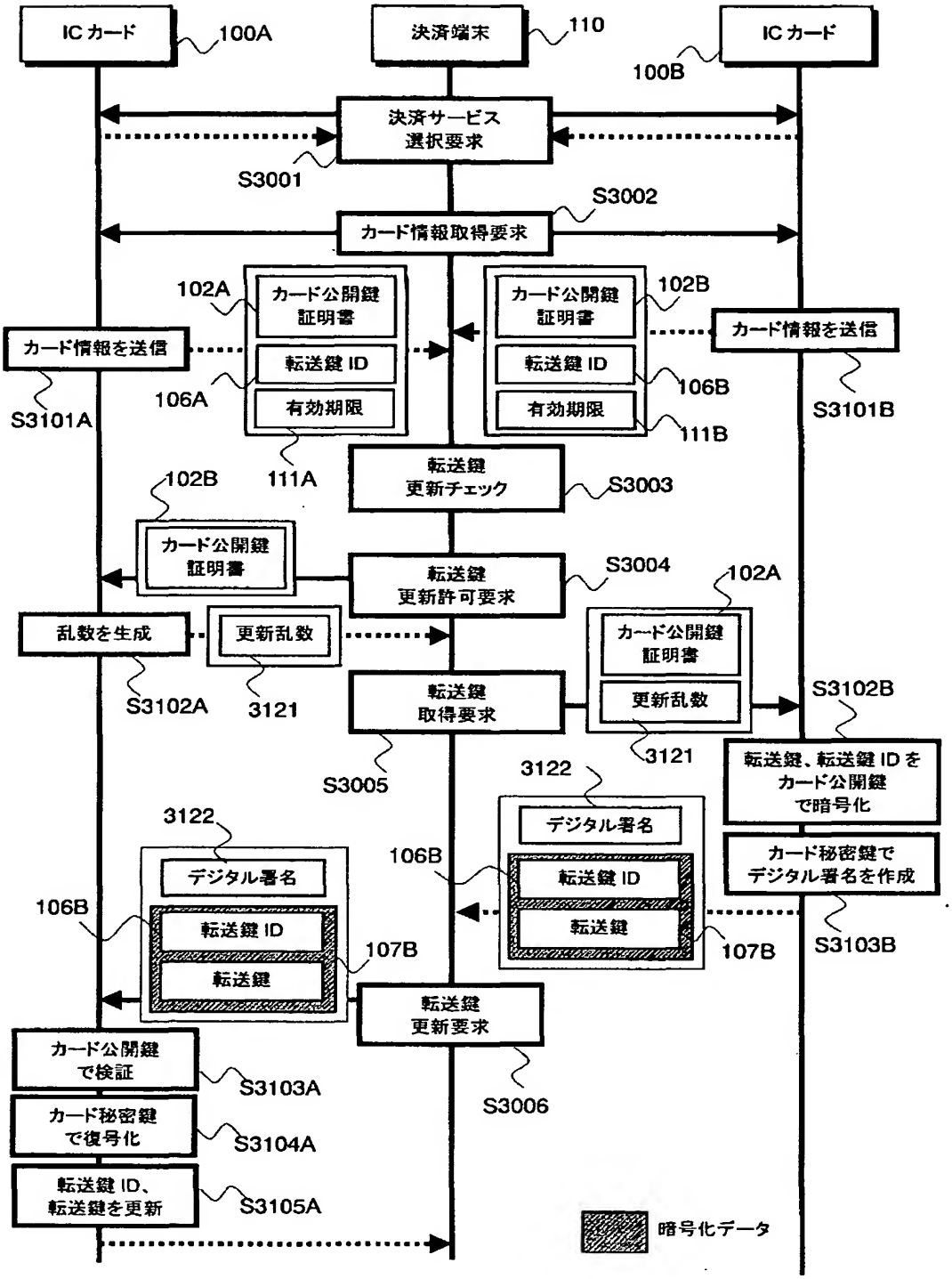
【図６】

図 6


鍵情報
204A
CA 公開鍵
101
カード公開鍵証明書
102A
カード秘密鍵
103A
転送鍵 ID
106A
転送鍵
107A
転送鍵 ID 上限値
112A

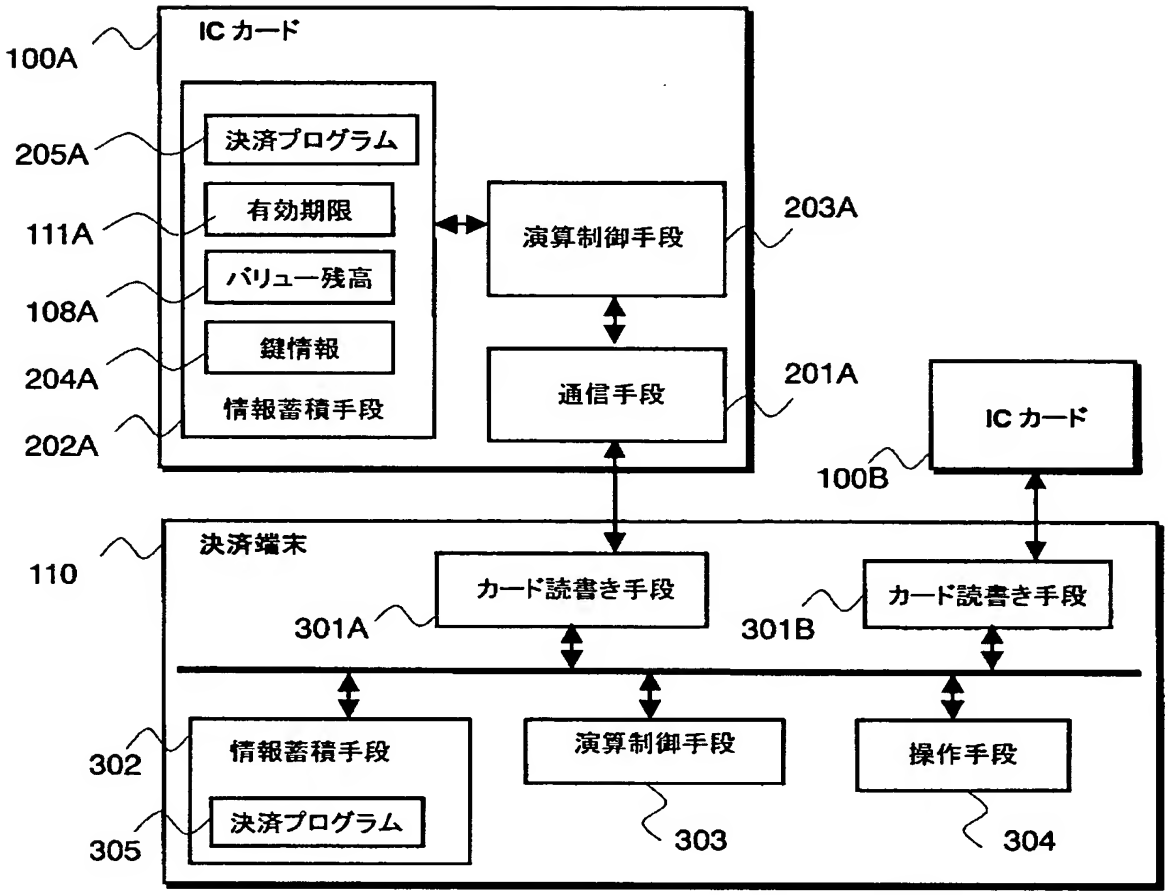
【図７】

図 7


ICカード
100A
決済端末
110
ICカード
100B
決済サービス
選択要求
S3001
S3002
カード情報取得要求
102A
カード公開鍵
証明書
転送鍵 ID
有効期限
106A
111A
102B
カード公開鍵
証明書
転送鍵 ID
有効期限
106B
111B
カード情報を送信
S3101A
カード情報を送信
S3101B
転送鍵
更新チェック
S3003
102B
カード公開鍵
証明書
転送鍵
更新許可要求
S3004
102A
乱数を生成
更新乱数
S3102A
3121
カード公開鍵
証明書
更新乱数
転送鍵
取得要求
S3102B
3121
S3005
3122
デジタル署名
転送鍵 ID
転送鍵
106B
107B
転送鍵、転送鍵 ID を
カード公開鍵
で暗号化
カード秘密鍵で
デジタル署名を作成
S3103B
3122
デジタル署名
転送鍵 ID
転送鍵
106B
107B
転送鍵
更新要求
S3006
カード公開鍵
で検証
S3103A
カード秘密鍵
で復号化
S3104A
転送鍵 ID、
転送鍵を更新
S3105A
暗号化データ

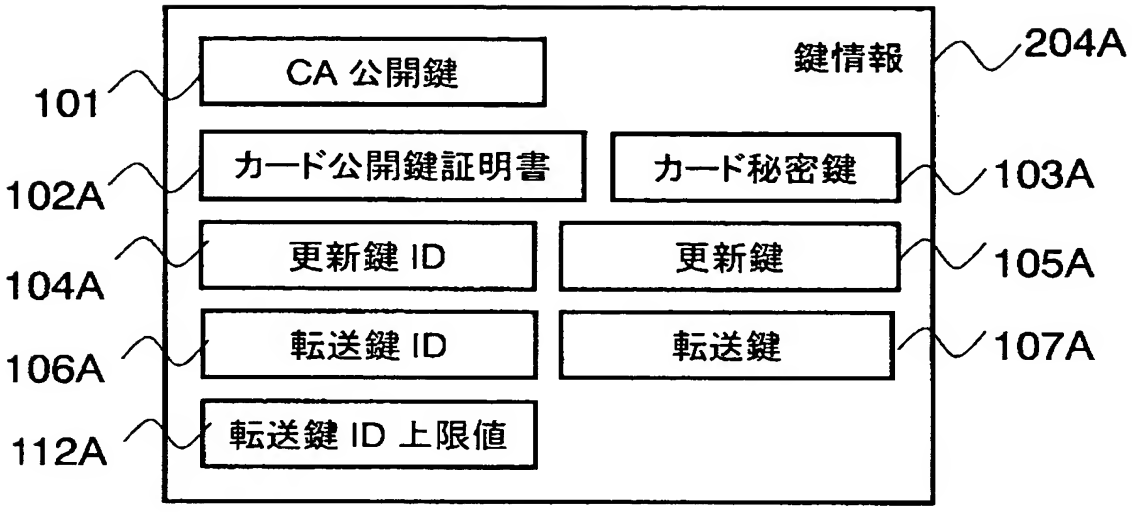
【図８】

図 8


ICカード
100A
決済プログラム
205A
有効期限
111A
バリュー残高
108A
鍵情報
204A
情報蓄積手段
202A
演算制御手段
203A
通信手段
201A
ICカード
100B
決済端末
110
カード読書き手段
301A
カード読書き手段
301B
情報蓄積手段
302
決済プログラム
305
演算制御手段
303
操作手段
304

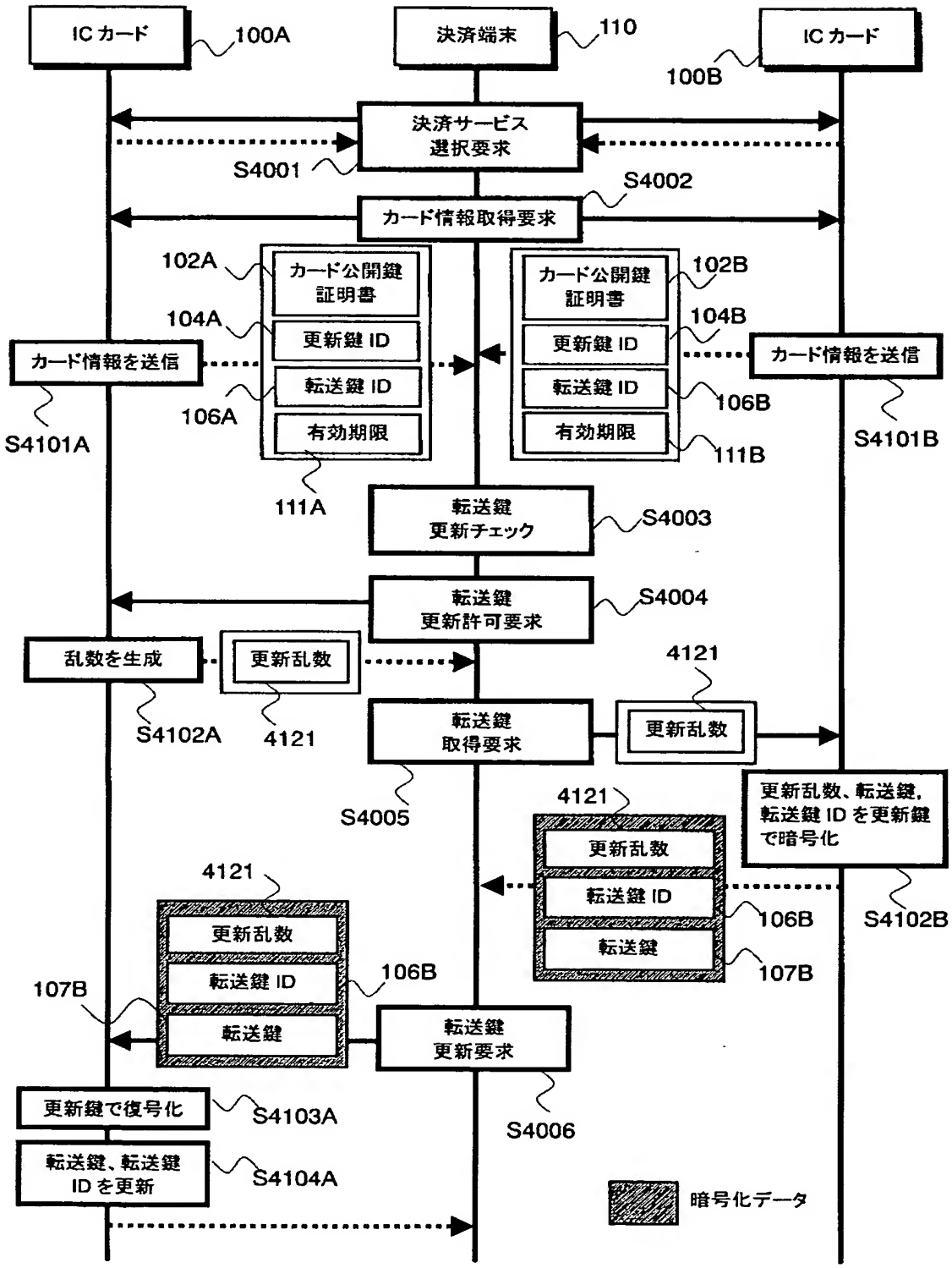
【図９】

図 9


CA 公開鍵
鍵情報
204A
101
カード公開鍵証明書
カード秘密鍵
102A
103A
更新鍵 ID
更新鍵
104A
105A
転送鍵 ID
転送鍵
106A
107A
転送鍵 ID 上限値
112A

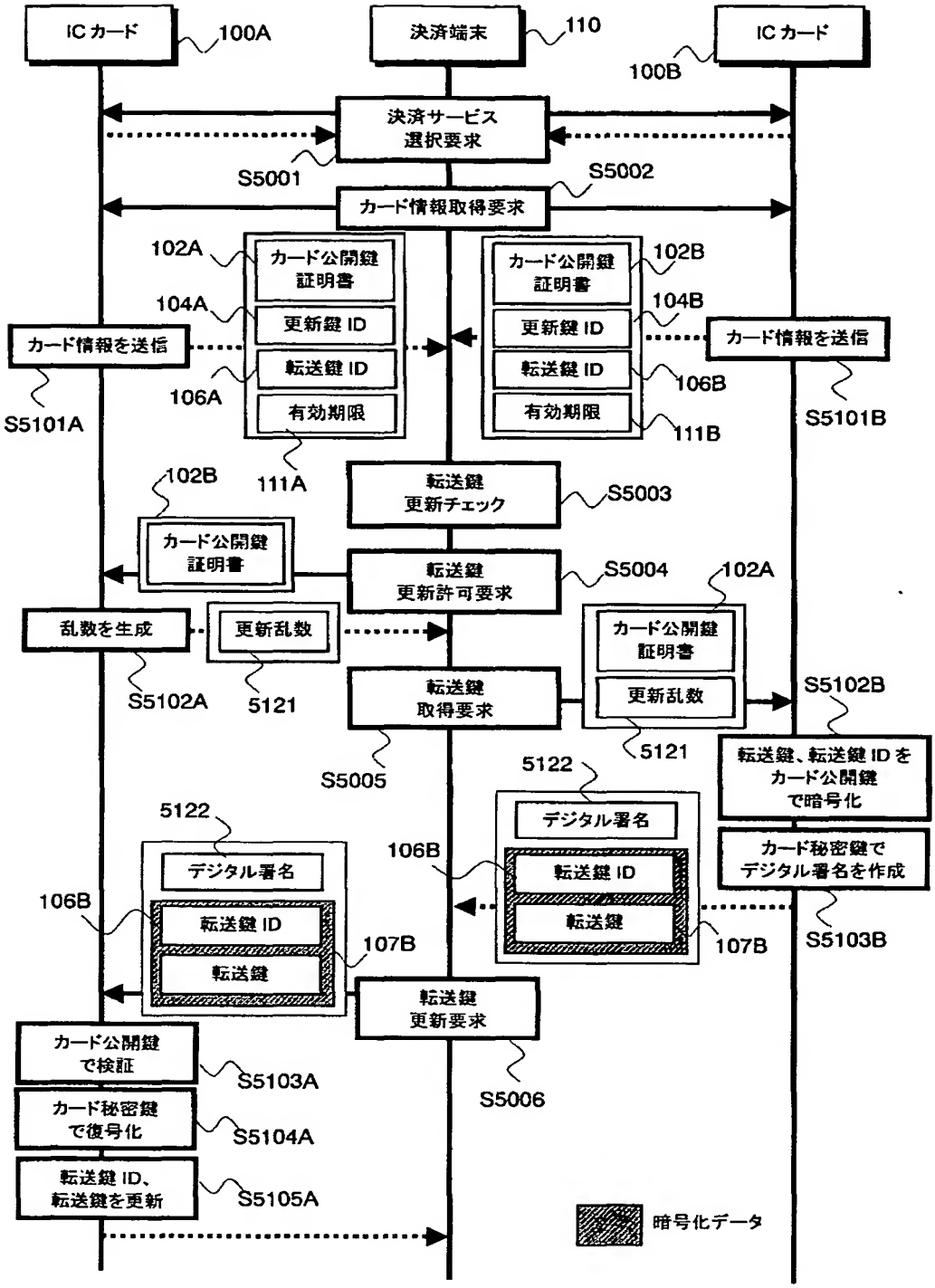
【図１０】

図 10


ICカード
100A
決済端末
110
ICカード
100B
決済サービス選択要求
S4001
S4002
カード情報取得要求
102A
カード公開鍵証明書
104A
更新鍵ID
転送鍵ID
106A
有効期限
111A
カード情報を送信
S4101A
102B
カード公開鍵証明書
104B
更新鍵ID
転送鍵ID
106B
有効期限
111B
カード情報を送信
S4101B
転送鍵更新チェック
S4003
転送鍵更新許可要求
S4004
乱数を生成
更新乱数
S4102A
4121
4121
転送鍵取得要求
更新乱数
S4005
4121
更新乱数
転送鍵ID
106B
転送鍵
107B
更新乱数、転送鍵、転送鍵IDを更新鍵で暗号化
S4102B
4121
更新乱数
転送鍵ID
106B
転送鍵
107B
転送鍵更新要求
S4006
更新鍵で復号化
S4103A
転送鍵、転送鍵IDを更新
S4104A
暗号化データ

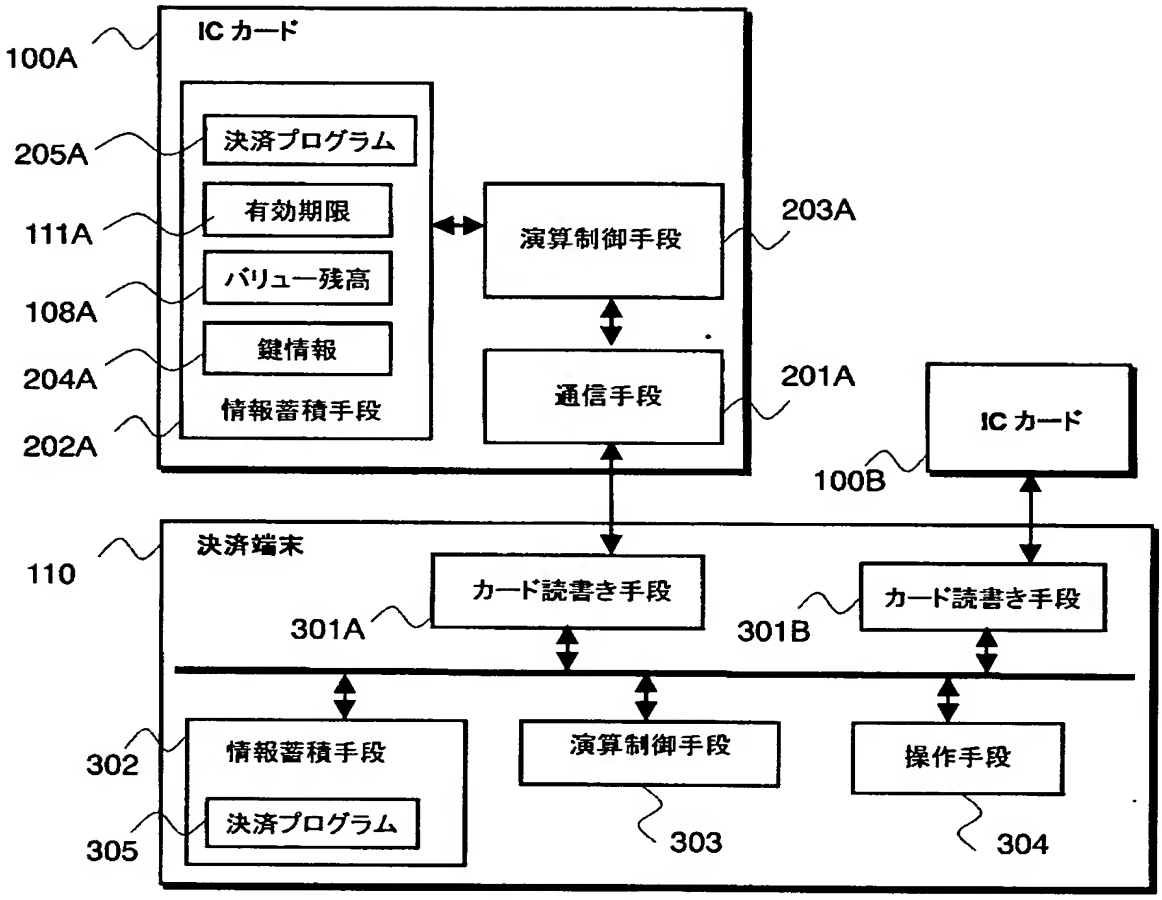
【図１１】

図 11


ICカード
100A
決済端末
110
ICカード
100B
決済サービス選択要求
S5001
S5002
カード情報取得要求
102A
カード公開鍵証明書
104A
更新鍵ID
転送鍵ID
106A
有効期限
111A
102B
カード公開鍵証明書
104B
更新鍵ID
転送鍵ID
106B
有効期限
111B
カード情報を送信
S5101A
カード情報を送信
S5101B
転送鍵更新チェック
S5003
102B
カード公開鍵証明書
転送鍵更新許可要求
S5004
102A
カード公開鍵証明書
更新乱数
乱数を生成
S5102A
更新乱数
5121
転送鍵取得要求
S5005
5121
S5102B
転送鍵、転送鍵IDをカード公開鍵で暗号化
5122
デジタル署名
106B
転送鍵ID
転送鍵
107B
カード秘密鍵でデジタル署名を作成
S5103B
5122
デジタル署名
106B
転送鍵ID
転送鍵
107B
転送鍵更新要求
S5006
カード公開鍵で検証
S5103A
カード秘密鍵で復号化
S5104A
転送鍵ID、転送鍵を更新
S5105A
暗号化データ

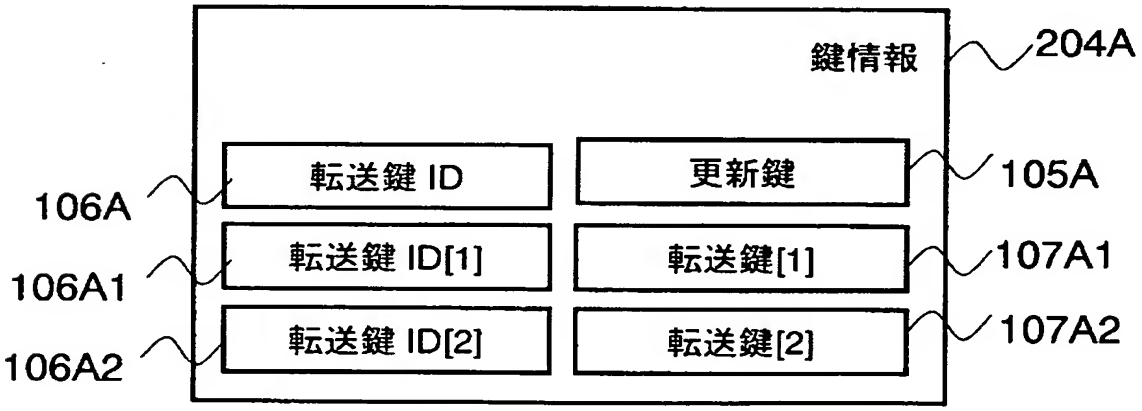
【図１２】

図 12



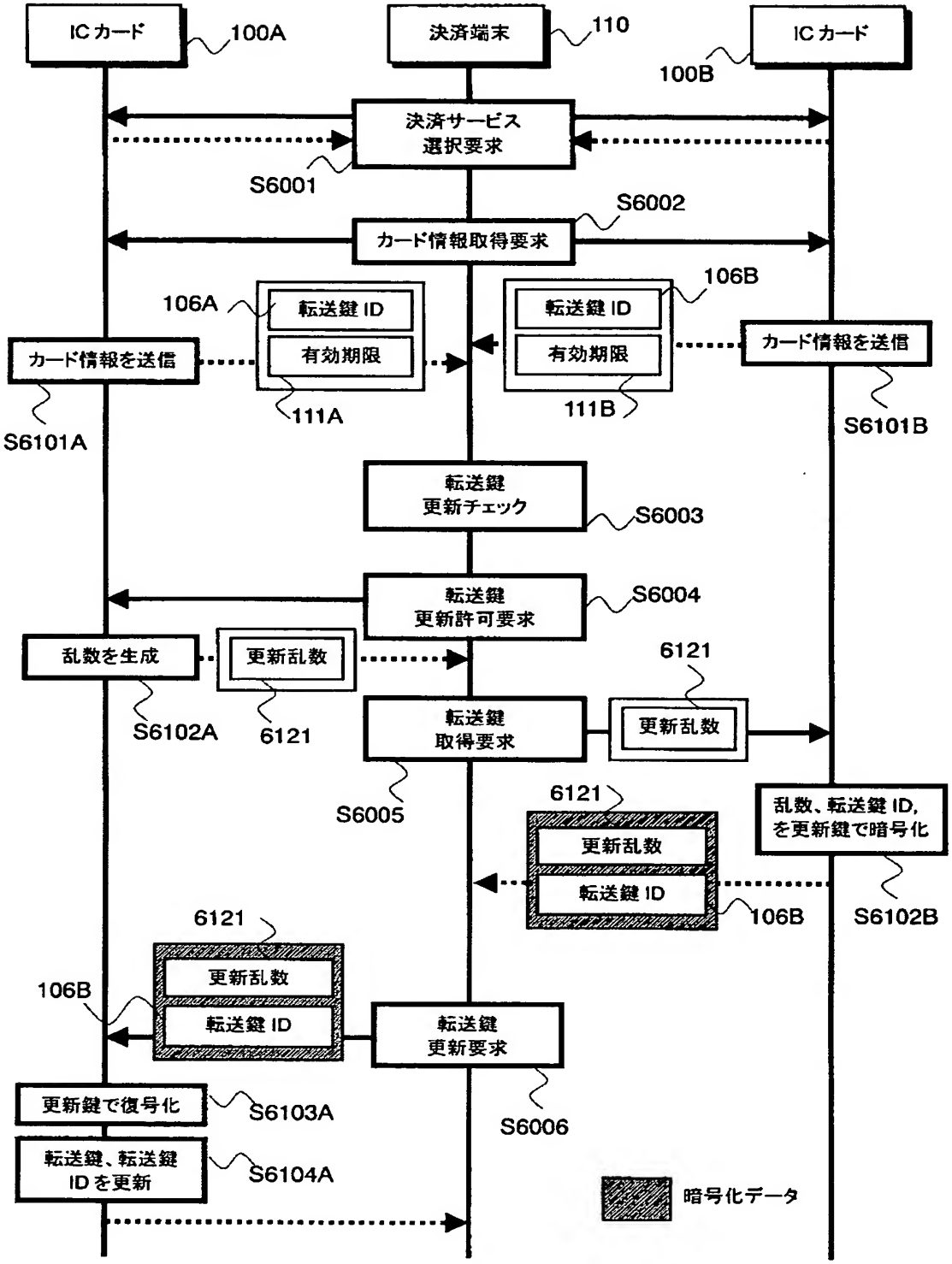
【図１３】

図 13



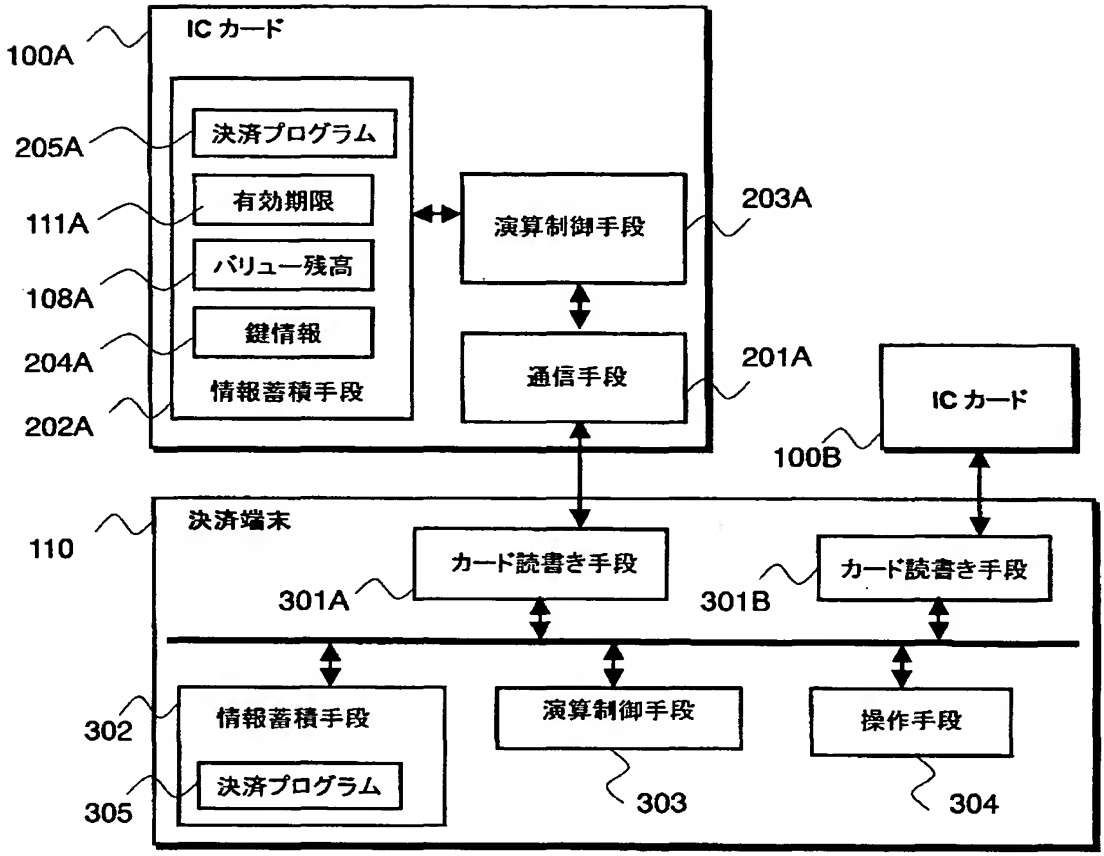
【図１４】

図 14


ICカード
100A
決済端末
110
ICカード
100B
決済サービス
選択要求
S6001
S6002
カード情報取得要求
106A
転送鍵 ID
有効期限
111A
106B
転送鍵 ID
有効期限
111B
カード情報を送信
S6101A
カード情報を送信
S6101B
転送鍵
更新チェック
S6003
転送鍵
更新許可要求
S6004
乱数を生成
更新乱数
S6102A
6121
6121
転送鍵
取得要求
更新乱数
S6005
6121
更新乱数
転送鍵 ID
106B
乱数、転送鍵 ID,
を更新鍵で暗号化
S6102B
6121
更新乱数
106B
転送鍵 ID
転送鍵
更新要求
S6006
更新鍵で復号化
S6103A
転送鍵、転送鍵
IDを更新
S6104A
暗号化データ

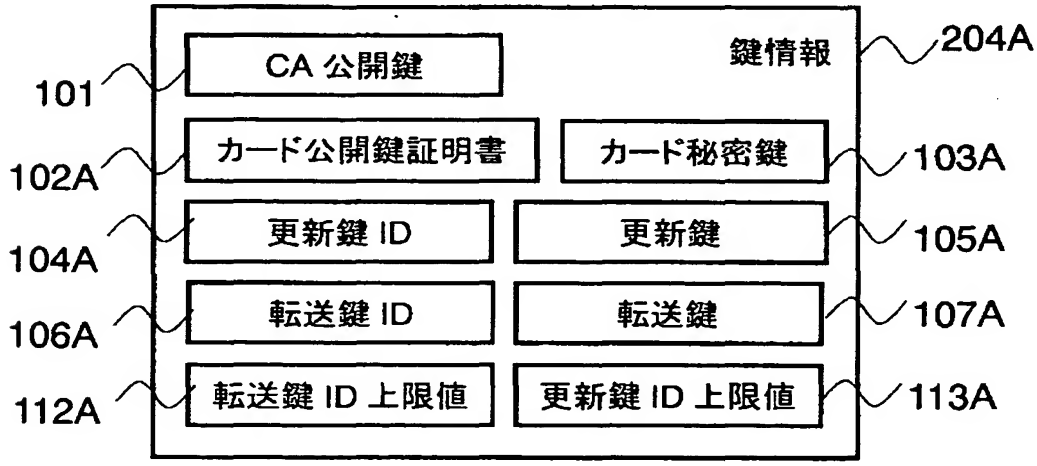
【図１５】

図 15



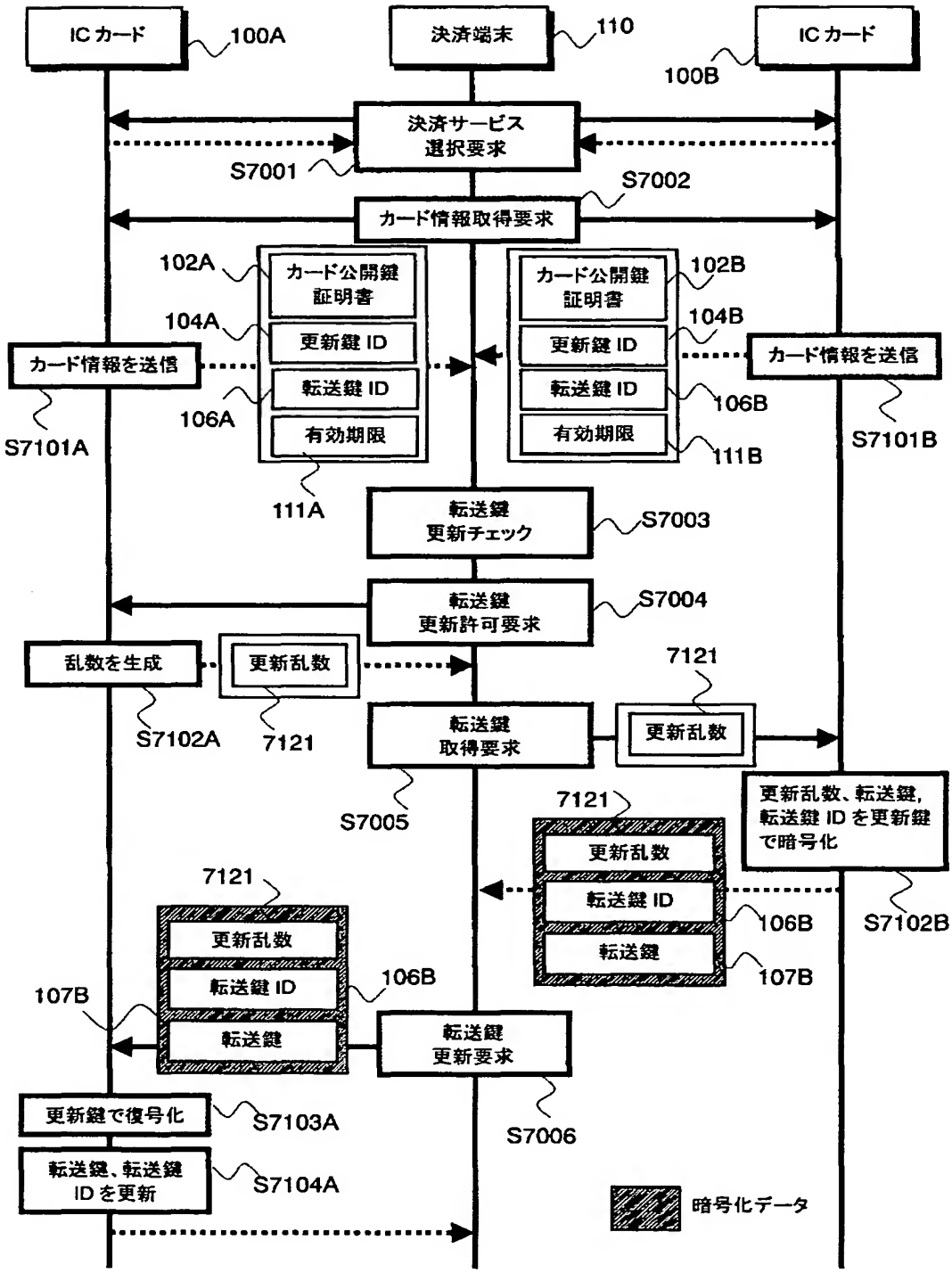
【図１６】

図 16



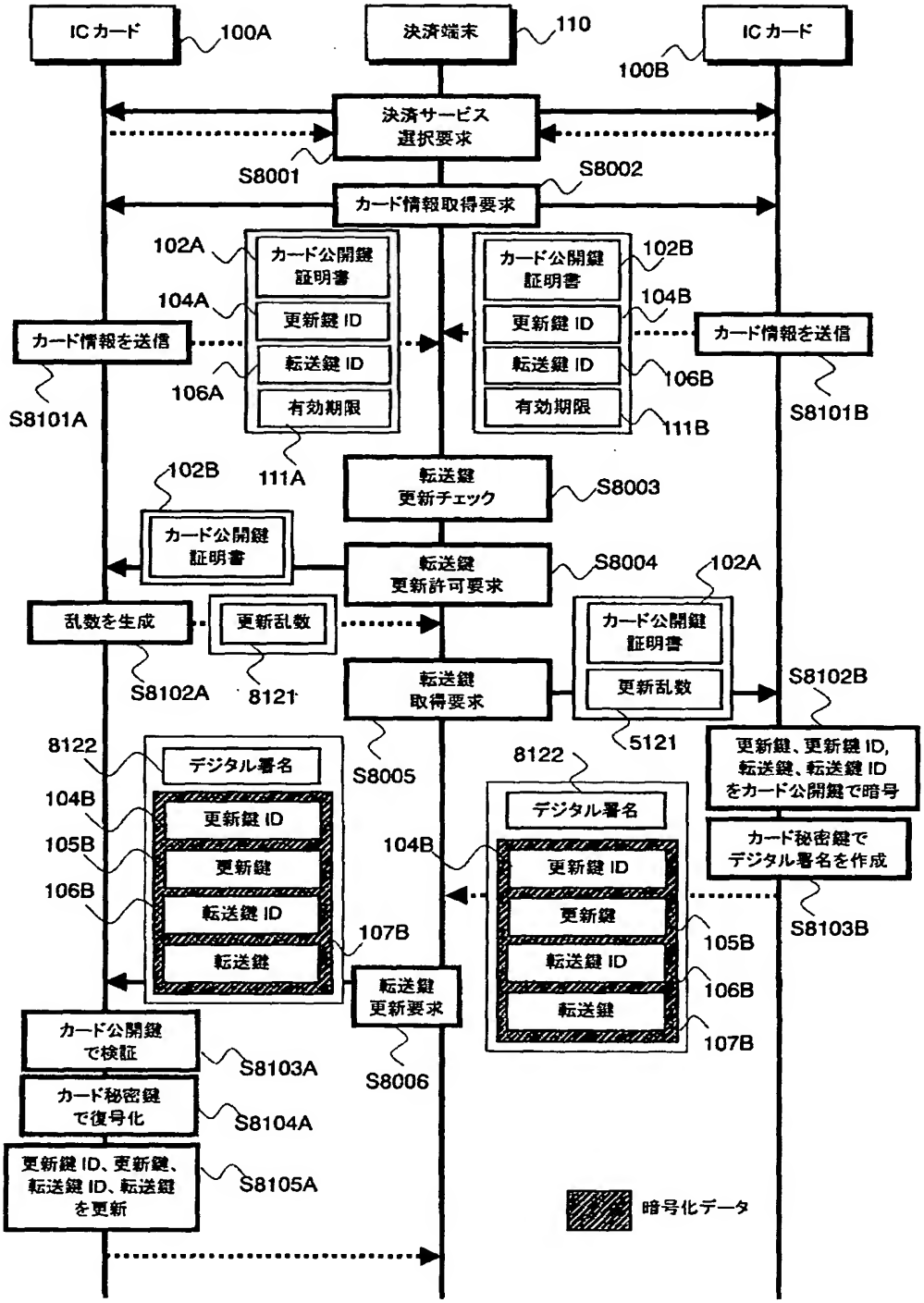
【図１７】

図 17


ICカード
100A
決済端末
110
ICカード
100B
決済サービス選択要求
S7001
S7002
カード情報取得要求
102A
カード公開鍵証明書
104A
更新鍵 ID
転送鍵 ID
106A
有効期限
111A
102B
カード公開鍵証明書
104B
更新鍵 ID
転送鍵 ID
106B
有効期限
111B
カード情報を送信
S7101A
カード情報を送信
S7101B
転送鍵更新チェック
S7003
転送鍵更新許可要求
S7004
乱数を生成
S7102A
更新乱数
7121
7121
転送鍵取得要求
更新乱数
S7005
更新乱数、転送鍵，転送鍵 ID を更新鍵で暗号化
S7102B
7121
更新乱数
転送鍵 ID
106B
転送鍵
107B
7121
更新乱数
転送鍵 ID
106B
転送鍵
107B
転送鍵更新要求
S7006
更新鍵で復号化
S7103A
転送鍵、転送鍵 ID を更新
S7104A
暗号化データ

【図１８】

図 18


ICカード
100A
決済端末
110
ICカード
100B
決済サービス選択要求
S8001
S8002
カード情報取得要求
102A
カード公開鍵証明書
104A
更新鍵 ID
転送鍵 ID
106A
有効期限
111A
カード情報を送信
S8101A
102B
カード公開鍵証明書
104B
更新鍵 ID
転送鍵 ID
106B
有効期限
111B
カード情報を送信
S8101B
転送鍵更新チェック
S8003
102B
カード公開鍵証明書
転送鍵更新許可要求
S8004
102A
乱数を生成
更新乱数
S8102A
8121
転送鍵取得要求
カード公開鍵証明書
更新乱数
S8102B
5121
更新鍵、更新鍵 ID、転送鍵、転送鍵 ID をカード公開鍵で暗号
カード秘密鍵でデジタル署名を作成
S8103B
8122
デジタル署名
S8005
104B
更新鍵 ID
105B
更新鍵
106B
転送鍵 ID
107B
転送鍵
転送鍵更新要求
S8006
8122
デジタル署名
104B
更新鍵 ID
105B
更新鍵
106B
転送鍵 ID
107B
転送鍵
カード公開鍵で検証
S8103A
カード秘密鍵で復号化
S8104A
更新鍵 ID、更新鍵、転送鍵 ID、転送鍵を更新
S8105A
暗号化データ

【書類名】要約書

【要約】

【課題】

ICカード間のバリュー転送に共通鍵暗号方式を用いた場合に、バリュー転送で使用する暗号鍵を容易に更新可能にすることで、システム全体のセキュリティを向上できるICカードおよび決済端末を提供することを目的とする。

【解決手段】

上記目的を達成するために本発明のICカードは、他のICカードと価値データを送受信するICカードであって、該価値データと、該価値データを更新するために用いる転送鍵と、該転送鍵を更新するために用いる更新鍵と、を蓄積する情報蓄積手段と、該他のICカードから送信された、該更新鍵を用いて暗号化された転送鍵を受信する通信手段と、該暗号化された転送鍵を該更新鍵を用いて復号化し、該復号化した転送鍵により該情報蓄積手段に蓄積されている転送鍵を更新する演算処理手段と、を備えることを特徴とする。

【選択図】図１

認定・付加情報

特許出願の番号	特願２００２－２２０６０２
受付番号	５０２０１１１９３５５
書類名	特許願
担当官	第八担当上席　００９７
作成日	平成１４年　７月３１日

＜認定情報・付加情報＞

【提出日】　平成14年 7月30日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　　東京都千代田区神田駿河台４丁目６番地
氏　名　　株式会社日立製作所